DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO DA EC GTS

Global Trusted Sign

Referência do Documento | DP02_GTS_V9

ÍNDICE

1. Referências	Regulamentação Europeia Nº 910/2014 ETSI 319 411-1 ETSI 319 412 ETSI 319 401 RFC 5280: Internet X.509 PKI - Certificate and CRL Profile, 2008 RFC 3647 - Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework, 2003. CA/Browser Forum: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates; ETSI TS 119 312: Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates
2. Documentos Associados	DP05_GTS - Declaração de Divulgação de Princípios da ROOT CA GTS
3. Lista de Distribuição	Partes interessadas da hierarquia de confiança da GTS
4. Histórico do Documento	31-07-2017 | Versão 1 12-09-2017 | Versão 2 29-12-2017 | Versão 3 05-03-2018 | Versão 4 08-03-2018 | Versão 5 09-01-2019 | Versão 6 02-05-2020 | Versão 7 24-06-2020 | Versão 8 17-09-2020 | Versão 9
5. Classificação do Documento	D | Público

6. Registo da Revisão

N.º da Versão	**Elaborado**	**Aprovado**	**Motivo**
	17-09-2020	**17-09-2020**	
9	**AdmSeg**	**Grupo de Gestão**	Atualização de registos de colaborador do Grupo de Confiança da GTS
	Sandra Mendes y Fernández	Tolentino de Deus Faria Pereira	
	Assinado com Assinatura Digital Qualificada por: SANDRA MENDES Y FERNÁNDEZ Data: 17-09-2020 17:54:21	Assinado com Assinatura Digital Qualificada por: TOLENTINO DE DEUS FARIA PEREIRA ACIN-iCloud Solutions, Lda Data: 17-09-2020 17:56:18	

7. Introdução

7.1. Âmbito

O presente documento tem por objetivo definir os procedimentos e práticas utilizadas pela Global Trusted Sign, enquanto prestadora qualificada de serviços de confiança no âmbito do regulamento 910/2014 (adiante designada por GTS), no suporte à atividade de emissão de certificados qualificados da Entidade Certificadora da GTS (adiante designada por EC GTS).

7.2. Público-Alvo

O presente documento apresenta-se disponível publicamente e é destinado a todos os participantes que se relacionem, de alguma forma, com a Entidade Certificadora da GTS.

7.3. Estrutura do Documento

No âmbito da presente declaração de práticas assume-se que o leitor é conhecedor dos conceitos de criptografia, infraestruturas de chave pública e assinatura eletrónica. Caso esta situação não se verifique, recomenda-se o estudo prévio acerca dos referidos tópicos, permitindo assim uma melhor compreensão do presente documento.

De forma a facilitar a leitura e consequente análise deste documento com as práticas difundidas e recomendadas internacionalmente, optou-se por incluir todas a secções estabelecidas no índice da norma "ETSI EN 319 411-1 v1.1.1. Policy and Security Requirements for Trust Service Providers issuing certificates; Part 1: General Requirements", pelo que se não houver nada designado sobre o assunto, será incluída a expressão "nada a assinalar".

Os acrónimos e definições estão definidos no Anexo A do presente documento.

8. Enquadramento

O presente documento de Declaração de Práticas de Certificação, ou DPC especifica os requisitos de segurança, políticas e práticas aplicáveis pelo prestador qualificado de serviços de confiança que emita certificados. As políticas e requisitos de segurança encontram-se definidos em termos de requisitos para a gestão do ciclo de vida dos certificados qualificados em conformidade com as políticas de certificados existentes.

Este documento respeita e implementa as seguintes normas:

- Regulamento (UE) N.º 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE
- ETSI EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements, v1.2.0

- ETSI EN 319 411-2: Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates, v1.1.1
- ETSI EN 319 401 v2.1.1: General policy requirements for Trusted Service Providers
- RFC 3647 - Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework, 2003.

As políticas da EC GTS têm por base as políticas definidas na norma ETSI EN 319 411-1, nomeadamente:

- Assinatura Qualificada e Selos Eletrónicos:
  - [NCP+] Normalized Certificate Policy requiring a secure cryptographic device
  - OID = 0.4.0.2042.1.2
- Autenticação de Sítios Web – *Organization Validation*:
  - [OVCP] Organizational Validation Certificate Policy
  - OID = 0.4.0.2042.1.7
- Autenticação de Sítios Web – *Extended Validation*:
  - [EVCP] Extended Validation Certificate Policy
  - OID = 0.4.0.2042.1.4

A GTS não tem suporte para o serviço de "cross-certificates".

O presente documento é a Declaração de Práticas de Certificação da EC GTS cujo OID associado é 1.3.6.1.4.1.50302.1.1.1.2.1.0, enquanto o OID associado às Políticas de Certificados da EC GTS são 1.3.6.1.4.1.50302.1.1.2.2.1.0 e 1.3.6.1.4.1.50302.1.1.2.4.1.0:

Informação do Documento	
Nome do Documento	Declaração de Práticas de Certificação da EC GTS
Versão do Documento	9.0
Estado do Documento	Aprovado
OID	1.3.6.1.4.1.50302.1.1.1.2.1.0
Data de Emissão	17 de setembro de 2020
Validade	17 de setembro de 2021
Localização	https://pki.globaltrustedsign.com/index.html

Nota: As atualizações realizadas a este documento são realizadas sempre que existam alterações aos procedimentos, legais ou estatais, ou sempre que se justifique.

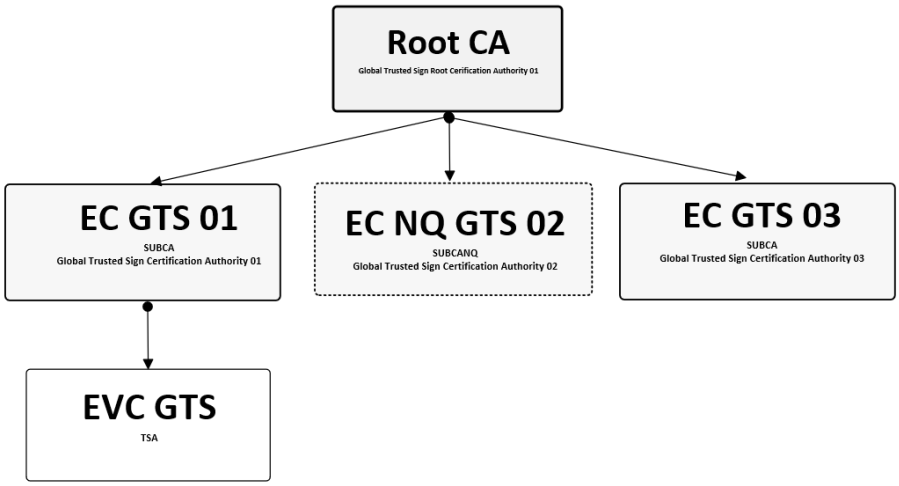
9. Participantes na Infraestrutura de Chave Pública

9.1. Entidades Certificadoras

A GTS, enquanto prestador qualificado de serviços de confiança, disponibiliza uma hierarquia de confiança credenciada pelo Gabinete Nacional de Segurança (http://www.gns.gov.pt/trusted-lists.aspx), conforme previsto na legislação portuguesa e europeia.

É composta por um conjunto de equipamentos, aplicações, recursos humanos e procedimentos indispensáveis para implementar os diversos serviços de certificação disponibilizados e garantir assim a adequada gestão do ciclo de vida dos certificados descritos no presente documento.

A hierarquia de confiança da GTS é composta pela Entidade Certificadora Raiz da GTS (ROOT CA GTS), a Entidade Certificadora da GTS (EC GTS), a Entidade Certificadora Não Qualificada da GTS (EC NQ GTS) e a Entidade Certificadora de Selos Temporais da GTS (EVC GTS). Estas entidades certificadoras estão descritas nos pontos 9.1.1, 9.1.2 e 9.1.3 do presente documento e encontram-se ilustradas de seguida:



Legenda:

1 – **Root CA GTS** - Entidade Certificadora Raiz da GTS
2 – **EC GTS 01** – Entidade Certificadora da GTS
3 – **EC NQ GTS 02** – Entidade Certificadora Não Qualificada da GTS
4 – **EVC GTS** – Entidade Certificadora de Validação Cronológica da GTS
5 – **EC GTS 03** – Entidade Certificadora da GTS

9.1.1. Entidade Certificadora Raiz da GTS (ROOT CA GTS)

A ROOT CA GTS é uma entidade certificadora credenciada pelo Gabinete Nacional de Segurança, de acordo com o Regulamento (UE) N.º 910/2014, estando deste modo habilitada, legalmente, a emitir certificados para Entidades Certificadoras Subordinadas.

O certificado da ROOT CA GTS:

Informação do Certificado	
Nome Distinto	CN = Global Trusted Sign Root Certification Authority 01, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT
Algoritmo de Assinatura	Sha256RSA
Nº de Série	7d 9f 44 7c b2 77 97 a8 59 57 bf 11 dd 8f 99 f5
Validade	01/07/2017 a 01/07/2037
Marca Digital	70 d1 2e f7 f5 90 18 87 47 88 42 c6 4e 05 ef 2c 0a 63 92 9d
Emissor	CN = Global Trusted Sign Root Certification Authority 01, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT

9.1.2. Entidade Certificadora da GTS (EC GTS)

A Entidade Certificadora da GTS emite:

1. **Certificados qualificados para autenticação de sítios Web (SSL/TLS)**

   Os serviços de autenticação de sítios web fornecem meios que dão aos visitantes de um sítio web a garantia de que existe uma entidade genuína e legítima responsável pelo sítio. Estes serviços contribuem para a criação de segurança e confiança na realização de negócios *online*, pois os utilizadores têm confiança nos sítios web que tenham sido autenticados, pela garantia de autenticidade, titularidade e confidencialidade da informação transacionada.

   A prática de emissão de certificados qualificados para autenticação de sítios web da EC GTS está em conformidade com os requisitos do CA/Browser fórum disponíveis em http://www.cabforum.org:

   - Organization Validation: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates
   - Extended Validation: Guidelines for the issuance and management of Extended Validation Certificates

Isso inclui a validação do domínio dos certificados requisitados (dono do domínio, domínio wild-card e CAA Records) conforme definido no CA/B Forum: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v1.6.3 capítulo 3.2.2.

Em caso de inconsistência entre esta DPC e estes Requisitos do CA/B Forum, os Requisitos assumem precedência.

2. Certificados para assinatura eletrónica qualificada

Os certificados para assinatura eletrónica qualificada permitem a criação de assinaturas digitais qualificadas em documentos eletrónicos com efeito legal equivalente ao de uma assinatura manuscrita, ao servir de prova da emissão de um documento eletrónico por determinada pessoa singular e confirma, pelo menos, o seu nome ou pseudónimo, bem como a integridade do documento.

3. Certificados para selos eletrónicos

Os certificados para selos eletrónicos permitem a criação de assinaturas digitais qualificadas em documentos eletrónicos com efeito legal equivalente ao de uma assinatura manuscrita, ao servir de prova da emissão de um documento eletrónico por determinada pessoa coletiva, certificando a origem e a integridade do documento.

Os certificados da EC GTS:

Informação do Certificado	
Nome Distinto	CN = Global Trusted Sign Certification Authority 001, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT
Algoritmo de Assinatura	Sha256RSA
Nº de Série	5D F5 55 01 8C 89 45 56 59 8D CF D9 13 3B 87 AB
Validade	11/08/2017 a 11/08/2023
Marca Digital	2b 30 32 d4 9d 12 74 af 30 ab a3 ec 29 a6 a0 25 ae f6 dc bc
Emissor	CN = Global Trusted Sign Root Certification Authority 01, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT

Informação do Certificado	
Nome Distinto	CN = Global Trusted Sign Certification Authority 03, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT
Algoritmo de Assinatura	Sha256RSA
Nº de Série	1e 0a 5a 4e b2 45 99 3c 5e b9 2f 31 48 db 0c f6
Validade	11/05/2020 a 11/05/2028
Marca Digital	60 2f 17 18 96 72 78 f5 88 4f 33 16 f2 65 9b c1 f3 cc b2 46
Emissor	CN = Global Trusted Sign Root Certification Authority 01, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT

9.1.3. Entidade Certificadora de Selos Temporais da GTS (EVC GTS)

A EVC GTS é uma entidade certificadora de validação cronológica habilitada a emitir selos temporais qualificados.

A monitorização do serviço de emissão de selos temporais tem o objetivo de detetar qualquer desvio maior que os requisitos impostos pela norma ETSI EN 319 421 (conforme explicado no capítulo 9.4.3). Serão monitorizados todos os offsets entre as máquinas que suportam o serviço de emissão de selos temporais com o objetivo de gerar alarmística relevante que será usada para tomar iniciativas corretivas.

Esta EVC GTS tem a responsabilidade de operar uma ou mais TSU (*time-stamping unit*) para a criação e assinatura de selos temporais em nome da GTS, cada uma com a sua chave distinta de assinatura, cujo relógio utilizado para emitir selos temporais, a infraestrutura é sincronizada temporalmente por relógio atómico interno e adicionalmente por duas fontes UTC alternativas:

- Royal Observatory of Belgium (ORB), Belgica, Bruxelas - ntp1.oma.be
- Observatoire de Paris (LNE-SYRTE), Paris, France - ntp-p1.obspm.fr

O certificado da EVC GTS:

Informação do Certificado	
Nome Distinto	CN = Global Trusted Sign Timestamping Authority 001, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT
Algoritmo de Assinatura	Sha256RSA
Nº de Série	04 bd 81 30 e4 ae 61 40 5a 99 43 db 7a 72 4f 47
Validade	02/03/2018 a 02/03/2023
Marca Digital	21 16 db 77 7e 72 fd 57 61 2a 24 27 8f d2 05 c8 bc fd a3 98
Emissor	CN = Global Trusted Sign Certification Authority 01, OU = Global Trusted Sign, O = ACIN iCloud Solutions, Lda, C = PT

9.1.4. Entidade Certificadora Não Qualificada da GTS (ECNQ GTS)

A Entidade Certificadora da GTS emite:

Certificados avançados para assinatura pela Entidade Certificadora Não Qualificada da Global Trusted Sign, enquanto prestadora de serviços de confiança, que cumprem os requisitos definidos no Regulamento (UE) Nº 910/2014 (no que for aplicável), no ETSI EN 319 401, v2.1.1 e ETSI EN 319 411-1, v1.1.1.

O certificado da EC NQ GTS:

Informação do Certificado	
Nome Distinto	CN = Global Trusted Sign NQ Certification Authority 02, OU = Global Trusted Sign, O = ACIN-iCloud Solutions, Lda, C = PT
Algoritmo de Assinatura	Sha256RSA
Nº de Série	7e 88 a8 ed 54 02 9f c6 5c 96 00 8e 0a cf bd c1
Validade	23/03/2019 até 23/03/2025
Marca Digital	7e 55 0f f3 8f 70 2e eb 5d 8f f0 e2 02 75 78 3f be 83 57 38
Emissor	CN = Global Trusted Sign Certification Authority 01, OU = Global Trusted Sign, O = ACIN iCloud Solutions, Lda, C = PT

1. **Certificados de assinatura e selos eletrónicos avançados**

Certificados emitidos para particulares e profissionais, permitindo a assinatura eletrónica de documentos (sem valor probatório) e a identificação eletrónica segura e unívoca de uma pessoa.

9.2. Autoridade de Registo

A Autoridade de Registo (RA) é a entidade responsável pela análise e avaliação dos pedidos de serviços da GTS, nomeadamente à veracidade dos documentos e validação da identidade dos titulares dos certificados e pedidos. Esta RA tem o direito de aprovar ou rejeitar os pedidos após a devida validação. Adicionalmente a RA tem autoridade para aprovar a revogação de certificados.

As Autoridades de Registo da Global Trusted Sign estão em conformidade com os requisitos estabelecidos neste documento e estão sujeitas a Auditorias Externas independentes, assim como Auditorias Internas realizadas Global Trusted Sign regularmente.

9.2.1. Autoridade de Registo Interna

No âmbito da Entidade de Certificação Global Trusted Sign, a autoridade de registo é executada pelos serviços internos da mesma, que têm responsabilidade de validação dos dados necessários, conforme explicitado nas Políticas especificas da Global Trusted Sign, para cada um dos serviços disponibilizados.

9.2.2. Autoridade de Registo Externa

A Global Trusted Sign, não dispõe de Autoridades de Registo Externas.

9.3. Subscritores e Titulares

No âmbito da presente declaração de práticas, os titulares podem ser:

- Uma pessoa singular;
- Uma pessoa singular em associação com uma pessoa coletiva;
- Uma pessoa coletiva (uma organização ou um departamento associado à organização);
- Um dispositivo ou sistema operado por ou em nome de uma pessoa singular ou coletiva.

Quando o subscritor é o próprio titular, este será diretamente responsável caso as suas obrigações não sejam completamente cumpridas.

Quando o subscritor está a agir em nome de um ou mais titulares a quem está associado, as responsabilidades do subscritor e do titular estão endereçadas na secção "Aceitação de Certificados".

O subscritor pode estar associado ao titular dos seguintes modos:

- Certificado para pessoa singular, o subscritor é:
  - A pessoa singular titular do certificado;
  - Uma pessoa singular com pseudónimo, desde que claramente indicado;

- Uma pessoa singular mandatada para representar o titular
- Uma entidade com a qual a pessoa singular está associada

- Certificado para pessoa coletiva, o subscritor é:
  - Qualquer entidade autorizada a representar a pessoa coletiva
  - Um representante legal da pessoa coletiva a subscrever certificados para as suas subsidiárias, ou departamentos

- Certificado para um dispositivo ou sistema operado por ou em nome de uma pessoa singular ou coletiva, o subscritor é:
  - A pessoa singular ou coletiva que opera o dispositivo ou sistema
  - Qualquer entidade autorizada a representar a pessoa coletiva
  - Um representante legal da pessoa coletiva a subscrever certificados para as suas subsidiárias, ou departamentos

No âmbito dos certificados para autenticação de sítios Web emitidos pela EC GTS, a pessoa singular ou coletiva poderá ser designada por patrocinador. Esta entidade aceita o certificado e é responsável pela sua correta utilização, bem como pela proteção e salvaguarda da respetiva chave privada.

9.4. Outros Participantes

9.4.1. Entidade Supervisora

A Entidade Supervisora é a entidade competente para a credenciação e fiscalização das entidades certificadoras prestadoras de serviços de confiança qualificados.

No panorama nacional, essa função é desempenhada pelo Gabinete Nacional de Segurança (GNS). A Entidade Supervisora contribui para a confiança nos certificados qualificados, pelas competências que exerce sobre as EC que os emite. No âmbito das suas funções, a Entidade Supervisora exerce os seguintes papéis relativamente às Entidades Certificadoras:

- **Notificação de intenção:** procedimento de aprovação dos serviços de confiança prestados pelos prestadores de serviços qualificados, com base numa avaliação feita a parâmetros tão diversificados como a segurança física, o hardware, software e os procedimentos de acesso e de operação;

- **Organismo de avaliação da conformidade:** enquanto organismo competente para realizar a avaliação da conformidade dos serviços de confiança prestados pelos prestadores de serviços qualificados;

- **Fiscalização:** Inspeções efetuadas para confirmar que tanto os prestadores qualificados de serviços de confiança como os serviços de confiança que prestam cumprem os requisitos estabelecidos pelo Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho.

9.4.2. Entidades Externas

A atividade dos prestadores de serviços que suportam a GTS no desempenho das suas funções enquanto prestadora qualificada de serviços de confiança é contratualizada de modo a garantir a atribuição formal das funções e responsabilidades de cada uma das partes, bem como o cumprimento das políticas e práticas instituídas na GTS.

9.4.3. Organismo de avaliação da conformidade

O Organismo de avaliação da conformidade (*Conformity Assessment Body* – CAB) é o organismo definido no artigo 2.º, n.º 13, do Regulamento (CE) n.º 765/2008, que é acreditado nos termos do mesmo regulamento como sendo competente para realizar a avaliação da conformidade de prestadores qualificados de serviços de confiança e dos serviços de confiança prestados por estes.

10. Utilização do Certificado

Os certificados emitidos pelo PKI da GTS são utilizados, pelos diversos titulares, sistemas, aplicações, mecanismos e protocolos, com o objetivo de garantir os seguintes serviços de segurança, nomeadamente:

a) Autenticação;
b) Confidencialidade
c) Integridade
d) Privacidade de Dados
e) Não Repúdio
f) Autenticidade

Estes serviços são obtidos com recurso à utilização de criptografia de chave pública, mediante a utilização da estrutura de confiança que a PKI da GTS disponibiliza.

As Partes Confiantes podem verificar a cadeia de confiança de um certificado emitido pela EC GTS, garantindo assim a autenticidade e identidade do titular.

Os certificados qualificados emitidos pela EC GTS de acordo com esta DPC são certificados qualificados em conformidade com os requisitos do regulamento (EU) 910/2014.

10.1. Utilização Adequada

a) Certificados qualificados de autenticação de sítios Web

Os certificados qualificados de autenticação de sítios Web emitidos pela EC GTS são utilizados, pelos diversos titulares, sistemas, aplicações, mecanismos e protocolos, com o objetivo de estabelecer comunicação de dados Web based através de protolocos SSL/TLS.

Os certificados qualificados de autenticação de sítios Web têm como objetivo:

- Identificar a entidade coletiva que controla um sítio web: fornece garantia razoável ao utilizador de um navegador Internet que o sítio web que o utilizador está a aceder é controlado por uma entidade coletiva que está identificada no certificado através do nome, sede social, inscrição no Instituto de Registos e Notariado, ou outra informação desambiguadora.

- Permitir comunicações cifradas com um sítio Web: facilita a troca de chaves de cifra de modo a permitir a comunicação de informação cifrada através da Internet, entre o utilizador de um navegador Internet e um sítio web.

Ao fornecer um processo de verificação de identidade mais fiável e informação da sede social da empresa, os certificados de *Extended Validation* (EV) podem ajudar a:

- Dificultar os ataques de phishing e outros de fraude de identidade que utilizam certificados

- Apoiar as empresas que possam ter sido o alvo de um ataque de phishing ou fraude de identidade ao disponibilizar uma ferramenta para a sua identificação perante os utilizadores

- Apoiar as forças de segurança nas suas investigações de phishing e outros ataques de fraude de identidade, apoiando, quando aplicável, o contacto, investigação, e ações legais contra o Titular.

b) Certificados para assinatura qualificada e selos eletrónicos

Os certificados qualificados de assinatura eletrónica e selos eletrónicos emitidos pela GTS são utilizados, pelos diversos titulares, sistemas, aplicações, mecanismos e protocolos, com o objetivo de permitir a assinatura probatória de documentos por pessoas singulares e coletivas

Os certificados para assinatura eletrónica qualificada devem ser utilizados para a criação de assinaturas digitais qualificadas em documentos eletrónicos com efeito legal equivalente ao de uma assinatura manuscrita.

Esta utilização permite servir de prova da emissão de um documento eletrónico por determinada pessoa singular e confirma, pelo menos, o seu nome ou pseudónimo, bem como a integridade do documento.

No caso dos certificados para selos eletrónicos, a utilização é análoga à dos certificados de assinatura qualificada, no entanto aplicam-se à prova da emissão por determinada pessoa coletiva, certificando a origem e a integridade do documento.

O subscritor é responsável pelo conteúdo de todas as transações realizadas através do serviço.

c) Certificados para assinatura e selos eletrónicos avançada

Os certificados digitais avançados oferecem um elevado nível de confiança, todavia não garantem o valor probatório dos certificados qualificados.

Estes certificados podem ser utilizados para:

- Realizar a sua autenticação online de forma segura;
- Assinar emails;
- Assinar documentos sem valor probatório legal.

10.2. Utilização não autorizada

Os certificados qualificados para autenticação de sítios Web emitidos pela EC GTS estão focados na identidade do Titular do certificado, e não no seu comportamento. Deste modo, um certificado de autenticação Web não dá quaisquer garantias sobre:

- O Titular identificado no certificado está efetivamente a prestar serviço;
- O Titular identificado no certificado está em conformidade com a legislação aplicável;
- Titular identificado no certificado é confiável, honesto ou ético na execução do seu negócio;
- Que é "seguro" estabelecer uma relação comercial com o Titular identificado no certificado.

O subscritor compromete-se a não utilizar o serviço para qualquer finalidade ilícita, a não provocar a interrupção do serviço, a não distribuir conteúdo que viole a privacidade, propriedade intelectual ou outros direitos proprietários de terceiros, ou para quaisquer outras finalidades que a GTS razoavelmente determine que sejam ilícitas, obscenas, difamatórias, fraudulentas, abusivas, ameaçadoras, prejudicais ou censuráveis.

Os certificados poderão ser utilizados noutros contextos apenas na extensão do que é permitido pela legislação aplicável.

Os certificados emitidos pela EC GTS não poderão ser utilizados para qualquer função fora do âmbito das utilizações descritas no ponto 10.1.

Os serviços qualificados de confiança oferecidos pela EC GTS, não foram concebidos nem estão autorizados a ser utilizados em atividades de alto risco ou que necessitem uma atividade isenta de falhas, como:

- Funcionamento de instalações hospitalares;
- Funcionamento de instalações nucleares;
- Controlo de tráfego aéreo;
- Controlo de tráfego ferroviário;

- Ou qualquer outra atividade onde uma falha possa levar à morte, lesões pessoais ou danos graves para o meio ambiente.

11. Gestão de Políticas

A gestão da declaração de práticas de certificação da EC GTS é da responsabilidade do grupo de Administração de Segurança da mesma.

Nome	Grupo de Administração de Segurança da EC GTS
Morada	ACIN iCloud Solutions Estrada Regional 104 Nº42-A 9350-203 Ribeira Brava Madeira Portugal
Correio Eletrónico	info@globaltrustedsign.com
Página Internet	https://www.globaltrustedsign.com
Telefone	707 451 451

A Declaração de Práticas de Certificação (DPC) deve ser aplicada internamente, bem como auditada pelo grupo de trabalho Auditor de modo a garantir a sua conformidade. Esta auditoria deve resultar num relatório, que deve ser submetido ao Grupo de Gestão da EC GTS, para aprovação.

11.1. Responsabilidades de Publicação e Repositório

A EC GTS disponibiliza um repositório, em ambiente web, de informação relativa às práticas adotadas e o estado dos certificados emitidos, nomeadamente:

- **Entidade Certificadora Raiz da GTS (ROOT CA GTS)**
    - Certificado da ROOT CA GTS;
    - Lista de Revogação de Certificados (LRC) da ROOT CA GTS;
    - Declaração de Práticas de Certificação (DPC) da ROOT CA GTS;
    - Políticas de Certificados (PC) da ROOT CA GTS;
    - Outra informação relevante.

- **Entidade Certificadora da GTS (EC GTS)**

- Certificado da EC GTS;
- Lista de Revogação de Certificados (LRC) da EC GTS;
- Declaração de Práticas de Certificação (DPC) da EC GTS;
- Políticas de Certificados da EC GTS;
- Outra informação relevante.

- **Entidade Certificadora de Selos Temporais da GTS (EVC GTS)**
  - Certificado da EVC GTS;
  - Declaração de Práticas de Certificação (DPC) da EVC GTS;
  - Políticas de Certificados da EVC GTS;
  - Outra informação relevante.

- **Entidade Certificadora Não Qualificada da GTS (EC GTS)**
  - Certificado da EC NQ GTS;
  - Lista de Revogação de Certificados (LRC) da NQ EC GTS;
  - Declaração de Práticas de Certificação (DPC) da EC GTS;
  - Políticas de Certificados da EC NQ GTS;
  - Outra informação relevante.

O repositório das diversas entidades certificadoras pode ser acedido 24x7 em:

- Repositório principal: https://pki.globaltrustedsign.com/index.html
- Repositório redundante: https://pki02.globaltrustedsign.com/index.html

Os repositórios serão atualizados sempre que haja uma alteração num dos documentos publicados.

A revogação dos certificados de uma da EC GTS poderá acontecer em vários casos:

- Comprometimento da chave privada do certificado da EC
- Cessação da atividade da TSP GTS
- Cessação da atividade desenvolvida pela presente EC

- Cessação ou comprometimento da EC que emitiu a EC em questão

A revogação da EC GTS acontece no prazo de máximo 7 dias depois de um dos casos acima mencionados acontecer.

A EC GTS efetua as seguintes publicações, com a seguinte periodicidade de publicação:

- O certificado da EC GTS é publicado após a sua emissão;
- A LRC é publicada de hora a hora, de modo a refletir qualquer alteração/revogação quase que de imediato.
- Novas versões ou alterações nas DPC e/ou respetivas Políticas de Certificados (PC), serão publicadas após a sua aprovação pelo Grupo de Gestão;

Foram implementados os seguintes mecanismos de controlo de acesso de segurança:

- Qualquer alteração à informação publicada no repositório é efetuada através de processos formais de gestão documental;
- A infraestrutura tecnológica que suporta o repositório e a sua publicação encontra-se em conformidade com as boas práticas de segurança da informação, incluindo os requisitos físicos bem como a gestão por uma equipa com as competências necessárias para a função;
- É garantido que o acesso à informação contida nos repositórios se efetua, apenas e só, em modo de leitura. Para tal, foram implementados mecanismos de segurança de forma a garantir que apenas pessoas autorizadas possam escrever ou modificar a informação contida nos repositórios.

11.2. Alterações às Políticas

Todos os documentos relacionados com a atividade da EC GTS, incluindo o presente documento (DPC), e quaisquer alterações subsequentes, tornam-se efetivos após publicação no repositório.

A EC GTS pode decidir em favor da eliminação ou emenda de um documento quando:

- Os seus conteúdos são considerados incompletos, imprecisos ou erróneos;
- Os seus conteúdos foram comprometidos.

O documento eliminado ou alvo de emenda é substituído por uma nova versão.

A validação da DPC e consequentes correções ou atualizações são da responsabilidade do Grupo de Administração de Segurança e devem:

- Ser publicadas sob a forma de novas versões desta DPC, substituindo qualquer DPC anteriormente definida.

- Determinar, após alterações na DPC, se identificadores dos objetos (OID) devem ser alvos de alguma alteração.

O Grupo de Gestão é a entidade responsável pela aprovação e autorização de modificações destes documentos.

Os subscritores são notificados por correio eletrónico quando se efetua uma mudança da DPC e que devem consultar a nova no repositório estabelecido.

Se a GTS determinar que a alteração ao identificador (OID) da política de certificados é necessária, a alteração deve conter os novos identificadores. De outra forma, as alterações não devem implicar uma mudança no identificador da política de certificados.

Todos os documentos relacionados com a atividade da EC GTS, e quaisquer alterações subsequentes, permanecerão ativos até publicação de nova versão ou alteração.

12. Identificação e Autenticação

12.1. Atribuição de Nomes

A EC GTS garante a emissão de certificados contendo um *Distinguished Name* (DN) X.509 a todos os titulares que submetem documentação contendo um nome verificável de acordo com o preconizado no RFC 5280.

A atribuição de nomes segue as convenções seguintes:

- Certificados de autenticação de sítios web é atribuído o nome qualificado do domínio e/ou do serviço de confiança, de acordo com a ETSI EN 319 412-4 v1.1.1;
- Certificados de assinatura qualificada para pessoa singular é atribuído o nome real do titular, de acordo com a ETSI EN 319 412-2 v2.1.1;
- Certificados de assinatura qualificada para pessoa singular em associação com uma pessoa coletiva é atribuído o nome do titular e a sua relação com a pessoa coletiva, de acordo com a ETSI EN 319 412-2 v2.1.1;
- Certificados de selos eletrónicos é atribuído o nome da pessoa coletiva, de acordo com a ETSI EN 319 412-3 v1.1.1.

A atribuição dos nomes cumpre os requisitos especificados nas políticas de certificados, estando nestas a identificação em cada uma das políticas:

Identificação da Política	Identificador único
Política de Certificado da Root CA	1.3.6.1.4.1.50302.1.1.2.1.1.0
Política de Certificado de Assinatura Eletrónica	1.3.6.1.4.1.50302.1.1.1.2.1.2
Política de certificado de Selos Eletrónicos	1.3.6.1.4.1.50302.1.1.1.2.1.3
Política de Certificado de SSL EV	1.3.6.1.4.1.50302.1.1.2.2.1.0
Política de Certificado de SSL OV	1.3.6.1.4.1.50302.1.1.1.2.1.1
Política de Selos Temporais	1.3.6.1.4.1.50302.1.1.2.3.1.0
Política de Certificados para assinaturas avançadas	1.3.6.1.4.1.50302.1.1.2.6.1.0
Política de Certificados de selos eletrónicos avançados	1.3.6.1.4.1.50302.1.1.2.7.1.0

Adicionalmente, a atribuição dos nomes cumpre os requisitos especificados nas políticas de certificados, para cada tipo de perfil apresentado.

Os vários tipos de certificados podem conter os seguintes campos no DN:

Atributo	Código	Regras
Country	C	Código do país do titular do certificado
Organization	O	Este campo corresponde à organização (ou equivalente) à qual o titular do certificado pertence.
Organization Unit	OU	Este campo corresponde informação relativa à unidade organizativa (ou equivalente) a que o titular do certificado pertence.
Common Name	CN	Nome único do titular do certificado. No caso dos servidores de sítios Web, este será designado pelo FQDN (CN = "FQDN".), sendo proibida a sua designação através do endereço IP. No caso dos certificados de assinatura qualificada, contém o nome do titular ou o seu pseudónimo. No caso dos certificados de selos eletrónicos, contém o nome da pessoa coletiva.
Serial Number	serialNumber	Segue as recomendações do ETSI EN 319 412.

A EC GTS assegura que os nomes utilizados nos certificados por ela emitidos identificam de uma forma significativa e clara os seus titulares, assegurando que o DN usado é apropriado para um dado titular e que a componente *Common Name* do DN o representa de forma a ser facilmente identificável

pelos interessados. Adicionalmente, a EC GTS garante a não existência de certificados emitidos por esta que, tendo o mesmo nome único, identifiquem entidades distintas.

Na EC GTS, existem controlos que garantem que o DN e o conteúdo da extensão *KeyUsage* são únicos, não ambíguos e referentes apenas a uma entidade não sendo também permitido o anonimato de titulares no processo de emissão de certificados.

É da responsabilidade da EC GTS atribuir e aprovar o DN, como também resolver quaisquer disputas que possam surgir com o DN atribuído.

O DN emitidos pela EC GTS têm em atenção as marcas registadas, não permitindo a utilização deliberada de nomes registados cuja entidade não possa provar ter direito à marca, podendo-se recusar a emitir o certificado com nomes de marcas registadas se concluir que outra identificação seja mais conveniente.

Antes da emissão do certificado, no procedimento de autenticação, a entidade/titular terá de apresentar documentos que demonstram o direito à utilização do DN requisitado.

No caso dos certificados para autenticação de sítios web, a EC GTS assegura que o utilizador possui a chave privada correspondente à chave pública que consta no pedido de certificado antes de proceder à sua emissão (por exemplo, envio por parte do requisitante do CSR – *Certificate Signing Request*).

12.2. Validação de Identidade Inicial

Para que os certificados qualificados possam ser emitidos na hierarquia de confiança da GTS, é obrigatório que a EC GTS verifique a identidade dos subscritores e titulares, e se aplicável outros atributos do titular, através da recolha de evidências diretas ou comprovativos de fontes adequadas e autorizadas, conforme descrito no Artigo 24. do Regulamento EU n.º 910/2014, no âmbito do cumprimento dos "requisitos aplicáveis aos prestadores qualificados de serviços de confiança", nomeadamente o seguinte "ao emitirem certificados referentes a serviços de confiança, os prestadores qualificados de serviços de confiança verificam, pelos meios adequados e nos termos da legislação nacional, a identidade e as eventuais características específicas da pessoa singular ou coletiva à qual é emitido o certificado qualificado. Para isso a GTS tem mecanismos para "provar e verificar a identidade das pessoas singulares ou coletivas que requeiram a produção do meio de identificação eletrónica".

A verificação da identidade dos subscritores e/ou titulares será efetuada pelo grupo de trabalho de Administradores e pode ser realizada das seguintes formas:

- De forma presencial, sempre com estando presentes neste ato dois administradores de registo (alínea a, do n.º 1, do artigo 24º do Reg.910/2014), ou;

- À distância, utilizando meios de identificação eletrónica, como a videoconferência através de software certificado para o efeito, para os quais tenha sido assegurada, antes da emissão do certificado qualificado, a presença física da pessoa singular ou de um representante autorizado da pessoa coletiva e que cumprem os requisitos estabelecidos no artigo 8.º do

regulamento 910/2014 relativamente aos níveis de garantia «substancial» ou «elevado» e o Despacho 154/2017 do GNS, (alínea b, do n.º 1, do artigo 24º do Reg.910/2014), ou

- Por meio de um certificado de assinatura eletrónica qualificada ou de um selo eletrónico qualificado emitido nos termos da alínea anterior (alínea c, d, do n.º 1, do artigo 24º do Reg.910/2014), apenas para cidadãos com cartão de cidadão português.

12.2.1. Identificação de pessoa singular

Se o titular é uma pessoa singular, a identidade poderá ser verificada através de:

1. Pessoa singular:
    - Nomes próprios e Apelido (de acordo com as práticas para identificação de pessoas)
    - Data e local de nascimento
    - Documento de identificação reconhecido que permita distinguir o titular de outros com o mesmo nome
    - Documento com valor probatório equivalente à presença física

2. Pessoa singular em associação com uma pessoa coletiva:
    - Nomes próprios e Apelido (de acordo com as práticas para identificação de pessoas)
    - Data e local de nascimento
    - Documento de identificação reconhecido que permita distinguir o titular de outros com o mesmo nome
    - Documento com valor probatório equivalente à presença física
    - Nome completo e dados sobre a pessoa coletiva
    - Evidência da associação da pessoa singular com a pessoa coletiva que irá aparecer nos atributos do certificado.

3. Pessoa Singular do Tipo Profissional
    - Nomes próprios e Apelido (de acordo com as práticas para identificação de pessoas);
    - Data e local de nascimento;
    - Documento de identificação reconhecido que permita distinguir o titular de outros com o mesmo nome;
    - Documento com valor probatório equivalente à presença física;
    - Indicação com evidência da Profissão que exerce;
    - N.º de Ordem a qual pertence com envio de evidência;
    - Organização / Entidade onde exerce a profissão com envio de evidência.

12.2.2. Identificação de pessoa coletiva

Se o titular é uma pessoa coletiva, a identidade poderá ser verificada através de:

1. Pessoa coletiva de representação

   - Nomes próprios e Apelido do requerente (de acordo com as práticas nacionais para identificação de pessoas)
   - Data e local de nascimento
   - Documento de identificação reconhecido nacionalmente que permita distinguir o titular de outros com o mesmo nome
   - Documento com valor probatório equivalente à presença física
   - Dados da pessoa coletiva:
     - Nome completo da pessoa coletiva
     - Morada
     - Identificação Fiscal (NIPC)
     - Código de Acesso da Certidão Permanente

   - Caso o requerente não seja um representante legal da pessoa coletiva, procuração de poderes de emissão do selo eletrónico.

2. Pessoa singular em associação com uma pessoa coletiva do tipo profissional:
   - Nomes próprios e Apelido (de acordo com as práticas nacionais para identificação de pessoas);
   - Data e local de nascimento
   - Documento de identificação reconhecido nacionalmente que permita distinguir o titular de outros com o mesmo nome;
   - Documento com valor probatório equivalente à presença física;
   - Nome completo e dados sobre a pessoa coletiva;
   - Evidência da associação da pessoa singular com a pessoa coletiva que irá aparecer nos atributos do certificado;
   - N.º de Ordem a qual pertence com envio de evidência;
   - Função/Cargo que desempenha;
   - Área / Departamento da organização à qual pertence.

12.2.3. Identificação de dispositivo ou sistema

O processo de registo e autenticação será assegurado pelo grupo de trabalho de Administradores de Registo com o objetivo de registar corretamente os utilizadores finais do certificado, usando todos

os meios necessários para uma identificação correta e legal do requerente. Entre as operações a realizar para atingir este objetivo contam-se as seguintes:

1. Verificar documentos oficialmente reconhecidos pelo Estado em que o subscritor (individual ou organização) está registado:
    - O nome completo;
    - Os dados de contato, incluindo o endereço de contato;
    - A sua identificação única legal.
2. A identificação deverá ser autenticada com provas identificativas que devem estar de acordo com as provisões seguintes:
    - Ser oficialmente reconhecidas na jurisdição em que o subscritor está registado;
    - Indicar o nome completo do subscritor e o seu endereço oficial;
    - Ter pelo menos uma prova de identidade que contenha uma fotografia do subscritor;
    - Indicar um número de registo único dentro da jurisdição em que tiver sido emitido;
3. A GTS verificará se cada candidato tem o direito ou privilégio para a obtenção do certificado em questão.

Para que os certificados qualificados de autenticação de sítios web com *extended validation* possam ser emitidos na hierarquia de confiança da GTS, é obrigatório que a EC GTS verifique a identidade e o endereço da entidade coletiva requerente, e que o endereço indicado seja o do pacto social, ou onde a sua atividade se realiza.

A validação inicial da identidade da entidade coletiva requerente através da análise da documentação submetida e através da comunicação com pelo menos um dos seguintes:

1. Verificação da criação, existência ou reconhecimento da entidade coletiva requerente através de uma agência governamental na jurisdição do requerente;

2. Uma base de dados terceira que seja periodicamente atualizada e seja considerada uma fonte fiável de dados;

3. Uma visita ao local pela EC GTS ou por um terceiro que esteja a agir enquanto agente da EC.

Caso o país de origem da organização seja Portugal, a validação inicial da identidade do requerente será efetuada através da análise da documentação submetida e através da verificação da criação, existência ou reconhecimento da organização requerente através do código de acesso à certidão permanente do Instituto de Registos e Notariado.

12.3. Proteção dos Registos

A EC GTS guardará os registos dos acordos assinados com os subscritores, incluindo os seguintes:

- Acordo dos termos e condições com o subscritor;
- Consentimento para a manutenção de registos por parte da GTS, com a informação usada no registo, bem como informação de subsequentes acontecimentos relativos ao acordo e ao seu objeto;
- Permissão para passar esta informação a terceiros sob certas condições;
- Permissão para passar informação sobre o estado dos certificados emitidos, ao abrigo do acordo, a terceiros não descriminados.

No processo de requisição de um certificado, a EC GTS seguirá os passos seguintes:

- Exigirá que uma entidade requerente de um certificado prepare e submeta os dados apropriados ao pedido como especificado nesta DPC;
- Verificará o Pedido lógico de Certificado para confirmar se este contém erros ou omissões de dados, de acordo com esta DPC;
- Verificará a unicidade do DN da entidade requisitante dentro da sua infraestrutura;
- Aceitará o pedido lógico de certificado vindo da entidade requisitante caso esta tenha sido validada;
- Rejeitará pedidos lógicos de certificado quando detetar chaves públicas repetidas.

A EC GTS guardará os documentos carregados para assinar, de acordo com o seguinte:

- Os documentos após assinados apenas ficam no portal da GTS, caso o titular assim o assinale;
- Durante o processo de assinatura dos documentos, os mesmos ficam guardados em locais seguros segregados de forma encriptada com algoritmo seguro AES e com 2 chaves privadas, sendo que, após esta execução são eliminados definitivamente.
- Pode o titular guardar os documentos no seu repositório no portal, de forma não encriptada para utilização posterior, sendo possível a qualquer momento serem eliminados definitivamente;

A capacidade de a pessoa agir em nome da organização candidata também será autenticada (no caso em que se trata de certificados qualificados para pessoas legais), através da apresentação de documentação em papel, indicando este facto.

12.4. Identificação e Autenticação para Pedidos de Renovação de Chaves

Muitas infraestruturas de chave pública permitem a atualização automática de certificados para um subscritor antes do fim do período de validade do certificado existente. Esta ação é conhecida como renovação de rotina, no entanto a renovação é tratada como um novo pedido de emissão.

12.5. Identificação e Autenticação para Pedidos de Revogação de Chaves

O Pedido de Revogação deve ser efetuado através do serviço disponibilizado para o efeito em https://www.globaltrustedsign.com, sendo que o certificado passará para o estado suspenso. Após receção e validação da documentação por parte da EC GTS, o estado do certificado será alterado para revogado e a respetiva LRC atualizada. Em caso de cancelamento do pedido, o estado de suspensão será levantado.

A verificação da identidade do requerente é efetuada conforme secção 12.2.

13. Requisitos Operacionais do Ciclo de Vida do Certificado

Os certificados emitidos pela PKI da GTS, são emitidos através do portal www.globaltrustedsign.com de forma autónoma pelo titular no caso de certificados qualificados de assinatura e selo eletrónico e pelo Administrador do Registo para os certificados SSL e certificados avançados, após o registo, validação da identidade dos titulares e respetiva aprovação do pedido de Certificado.

13.1. Pedido de Certificado

Os pedidos de subscrição de certificados podem ser submetidos pelos seguintes:

- O titular do certificado;
- Um representante do titular do certificado, devidamente autorizado e com poderes para o efeito;
- Uma pessoa coletiva que seja titular do certificado;
- Um representante da GTS.

13.2. Processamento do Pedido de Certificado

Um pedido de emissão de certificados à EC GTS inicia-se com o preenchimento de um formulário, desenhado para cada tipo de certificado suportado e com a aceitação dos termos e condições estabelecidos pela EC GTS, devidamente assinados pelo titular de forma manuscrita e que neste caso pressupõe o envio dos documentos originais por CTT para a GTS ou de forma digital, com recurso a assinatura qualificada.

Após a receção da documentação, dá-se início a um processo de validação da informação e identidade do titular e quando aplicável entidade requerente. Este processo é executado sempre por 2 Administradores de Registo, com o fim de verificar a autenticidade dos dados fornecidos, dependendo do tipo de certificado solicitado.

A GTS não utiliza entidades de registo externas para fornecimento do serviço de registo.

No caso dos certificados Web/SSL, o formulário deverá ser acompanhado aquando a sua submissão, de um CSR (Certificate Signing Request) que deve conter informação para os campos do certificado, que devem coincidir com os campos inseridos no formulário.

Nota: O pedido de certificado não implica a sua obtenção se o solicitante não cumprir os requisitos estabelecidos nesta DPC. Os pedidos efetuados aceites ou rejeitados serão arquivados e mantidos por um período de 7 anos de acordo com o CAB Fórum secção 5.5.2.

13.3. Emissão de Certificado

Este processo é executado por dois Administradores de Registo, recorrendo a dupla autenticação com o fim de verificar a autenticidade dos dados fornecidos, dependendo do tipo de certificado solicitado.

Os certificados são emitidos por interação da Entidade Certificadora com um módulo criptográfico em hardware (Hardware Secure Module - HSM), tendo por base o tipo de política de certificado aplicável. O certificado de chave pública é armazenado no HSM.

No caso dos certificados para autenticação de sítios web, o certificado emitido inicia a sua vigência no momento da sua emissão e o subscritor do certificado é notificado via correio eletrónico, sendo-lhe enviado, por este canal, o certificado de chave pública. O envio do certificado requer uma aceitação que é feita de acordo com a secção 13.4 Aceitação de certificado.

A GTS tem 60 minutos após validação da identidade e idoneidade do subscritos e boa cobrança para proceder com a emissão e envio do certificado de autenticação web.

Não serão aceites terminologias não reconhecidas pela ICANN (Internet Corporation for Assigned Names and Numbers), para aceitação de certificados de sítios web.

No caso dos certificados de assinatura qualificada ou selo eletrónico qualificados, a emissão do certificado é efetuada pelo titular do mesmo após verificação da identidade do titular no momento da emissão através de:

- Credenciais de acesso ao Portal da GTS
- Receção do código OTP para o email configurado no registo do titular

Os titulares dispõem de 30 dias para emitir qualquer tipo de certificado sob pena de ter que repetir a videoconferência.

Os Certificados avançados são emitidos pelos administradores de registo e ficam disponíveis para download na área pessoal do portal GTS, uma vez realizada a autenticação. Para a utilização do certificado será enviado por sms um pin, para o número de telemóvel identificado pelo próprio titular para o efeito aquando a realização da compra do produto. Este certificado pode ser descarregado quantas vezes for necessário

13.4. Aceitação de Certificados

Antes do envio do certificado de chave pública, o subscritor e titular terão de aceitar as condições de utilização do certificado, só assim é que certificado considera-se aceite.

Perante o certificado emitido, subscritor deve ser uma entidade consciente dos tópicos seguintes:

- O conhecimento das funcionalidades e conteúdo do certificado;
- O conhecimento dos direitos e responsabilidades.

A EC GTS não efetua a publicação de certificados emitidos, nem notifica outras entidades da emissão dos mesmos.

13.5. Uso do Certificado e Par de Chaves

Os titulares de certificados utilizam a sua chave privada apenas, e só, para o fim a que estas se destinam (conforme estabelecido no campo do certificado "keyUsage") e sempre com propósitos legais. A utilização do certificado é sempre da responsabilidade do seu titular.

A utilização do certificado apenas é permitida, e caso aplicável para o tipo de certificado em questão:

- A quem estiver designado no campo do certificado Subject;
- Depois de aceitar os termos e condições associados ao tipo de certificado;
- Enquanto o certificado se mantiver válido e não estiver na LRC da EC GTS.

13.6. Renovação de Certificados

Para realizar a renovação do seu certificado, e se as funções e informações para as quais o certificado inicial foi emitido se mantiverem, apenas terá de solicitar a renovação do seu certificado com os mesmos dados e efetuar pagamento de renovação seguindo as indicações que lhe serão enviadas pela GTS. Este processo obriga a uma nova geração de um par de chaves, e respetivo certificado.

Se um titular pretender renovar um certificado é desencadeado um procedimento para cada um dos seguintes casos:

Motivo para Renovação	Procedimento de Renovação
O certificado foi revogado	(*i*) Um novo par de chaves é gerado, e consequentemente um novo certificado é emitido com os mesmos campos exceto a chave pública.
O titular pretende prolongar a validade do certificado	(*i*) O antigo certificado é revogado. (*ii*) Um novo par de chaves é gerado, e consequentemente um novo certificado é emitido com os mesmos campos exceto a chave pública.
A informação que deu origem ao certificado sofre alterações	(*i*) O antigo certificado é revogado. (*ii*) Um novo par de chaves é gerado, e consequentemente um novo certificado é emitido com as alterações necessárias incluindo a nova chave pública.

A renovação de certificados utiliza os procedimentos de autenticação e identificação inicial (secção 12.2 Validação de Identidade Inicial), que resultam na geração de novos pares de chaves.

13.7. Renovação de Certificados com Geração de Novo Par de Chave

A renovação de certificados utiliza os procedimentos de autenticação e identificação inicial (secção 12.2. Validação de Identidade Inicial), que resultam na geração de novos pares de chaves.

13.8. Modificação de Certificados

A modificação de certificados para autenticação de sítios web não é suportada pela EC GTS.

13.9. Revogação de Certificados

A revogação de certificados são mecanismos a utilizar quando por algum motivo os certificados deixam de ser fiáveis, antes do período de finalização originalmente previsto.

Na prática, a revogação de certificados é uma ação através da qual, o certificado deixa de estar válido antes do fim do seu período de validade, perdendo, deste modo, a sua operacionalidade.

A suspensão de certificados não é suportada pela EC GTS.

13.9.1. Revogação de Certificados

Um certificado pode ser revogado por uma das seguintes razões:

- Cessação de funções;
- Roubo, extravio, destruição ou deterioração do dispositivo de suporte dos certificados;
- Incapacidade ou falecimento do titular;
- Inexatidões nos dados fornecidos;
- Comprometimento ou suspeita de comprometimento das chaves privada do titular;

- Comprometimento ou suspeita de comprometimento da senha de acesso ao certificado;
- Comprometimento ou suspeita de comprometimento das chaves privada da EC;
- Incumprimento por parte da EC ou titular das responsabilidades prevista na DPC;
- Sempre que haja razões credíveis que induzam que os serviços de certificação possam ter sido comprometidos, de tal forma que coloquem em causa a fiabilidade dos certificados;
- Por resolução judicial ou administrativa;
- Por vontade do próprio.

Um pedido de revogação pode ser efetuado de forma legítima por um dos seguintes intervenientes:

- O Titular (pessoa física);
- A Entidade Requerente do certificado;
- A GTS, no conhecimento de que:
  - Os dados constantes no certificado não correspondem à realidade;
  - O certificado não está na posse do titular.
- A Entidade Supervisora;
- Uma parte confiante, sempre que demonstre que o certificado foi utilizado com fins diferente dos previstos.

O Pedido de Revogação deve ser efetuado através do serviço disponibilizado para o efeito em https://www.globaltrustedsign.com. A EC GTS irá processar o pedido de revogação em 24 horas seguintes às da receção do pedido. Nesse intervalo de tempo, será verificada a identidade e autenticidade de quem solicitou a revogação do certificado. Após a confirmação da identidade e autenticidade do requerente, a TSP GTS tem 60 minutos, para transitar o estado do certificado para revogado.

Os certificados revogados podem ser consultados através da LRC da Entidade de Certificação da GTS.

13.10. Serviço sobre o estado do Certificado

As LRC podem ser acedidas em https://pki.globaltrustedsign.com/index.html, garantindo a sua disponibilidade 24 horas por dia, 7 dias por semana, exceto na ocorrência de alguma paragem de manutenção programada e devidamente comunicada às partes envolvidas.

O fim da subscrição de um certificado ocorre quando o prazo de validade é ultrapassado expirado ou o certificado é revogado, conforme RFC 3647.

13.10.1. Frequência de Emissão de CRL

Os estados dos certificados emitidos pela ROOT CA da GTS podem ser verificados através da consulta da sua CRL. Esta é emitida sempre que haja uma revogação dos certificados emitidos ou, na ausência de alterações no estado dos certificados, de forma trimestral. A disponibilização nos

repositórios é feita num período não superior a 30 minutos, sendo o seu download feito em menos de 10 segundos. De modo a garantir a sua disponibilidade, a CRL é disseminada nos seguintes repositórios:

https://pki.globaltrustedsign.com/root/gts_root_crl.crl

https://pki02.globaltrustedsign.com/root/gts_root_crl.crl

13.10.2. Outras Formas de Anúncio de Revogação

A Global Trusted Sign Root CA dispõe de serviços de validação OCSP do estado dos certificados de forma online.

Esse serviço poderá ser acedido em https://ocsp.globaltrustedsign.com

14. Controlos de Segurança Física, de Gestão e Operacionais

14.1. Controlos de Segurança Física

A EC GTS foi desenhada de forma a proporcionar um ambiente seguro capaz de proteger os sistemas que suportam a atividade da EC GTS. As operações da GTS são realizadas numa sala numa zona de alta segurança, dentro de um edifício que garante a existência de diversos níveis de segurança acessíveis apenas às pessoas que dele necessitem para desempenho das suas funções de confiança.

A GTS garante ainda que as suas zonas de alta segurança possuem todo o conjunto de características previstas, bem como os mecanismos necessários por forma a garantir as condições de segurança, no que concerne a:

- Localização física e tipo de construção;
- Acesso físico ao local;
- Energia e ar condicionado;
- Exposição à água / inundações;
- Prevenção e proteção face a incidentes/desastres tais como incêndios, inundações e semelhantes;
- Eliminação de resíduos;
- Salvaguarda dos suportes de informação.

Os suportes de informação sensível são armazenados, de forma segura, em cofres e de acordo com o tipo de suporte e classificação da informação. O acesso a estas zonas é restrito a pessoas fora do âmbito do grupo de confiança da GTS.

No final do seu ciclo de vida, documentos e materiais em papel que contenham informações críticas deverão ser eliminados através de métodos eficazes que não permitam a reconstrução dos mesmos.

Outros equipamentos de armazenamento (discos rígidos e afins) devem ser devidamente limpos, de modo a não seja possível recuperar alguma informação através de formatações seguras, ou proceder

à destruição física dos mesmos. No caso de periféricos criptográficos, estes devem ser destruídos segundo as instruções e recomendações dos respetivos fabricantes.

14.2. Controlos dos Processos

A atividade de emissão de certificados digitais da GTS, enquanto entidade certificadora de certificados qualificados, exige o cumprimento de um conjunto de normas europeias.

Estas mesmas normas definem um conjunto de grupos de trabalho, com competências, atividades e regras distintas, que deve ser garantido pela GTS.

Na GTS todos os elementos que tenham acesso ou que controlem operações criptográficas ou de autenticação estão inseridos num determinado grupo de trabalho dependendo das suas funções.

14.2.1. Grupo de Trabalho da Administração de Segurança (AdmSeg)

Responsabilidades: Responsáveis globais sobre segurança dos sistemas, nomeadamente, pela gestão e implementação das regras e práticas de segurança no âmbito dos serviços prestados pela GTS.

Descrição de Tarefas:

- Definição da documentação associada às práticas de segurança da informação da GTS
- Definição dos procedimentos relacionados com a gestão das chaves criptográficas
- Garantia de que toda a documentação associada à GTS se encontra atualizada, adaptada à realidade e armazenada de forma segura de acordo com a sua classificação
- Gestão da implementação das práticas e políticas de segurança, incluindo o controlo de acessos lógico e físico
- Gestão dos riscos associados aos serviços prestados pela GTS
- Monitorização dos eventos de segurança e gestão da alarmística associada a estes
- Participação e resposta aos incidentes de segurança
- Guarda dos artefactos sob a sua custódia

14.2.2. Grupo de Trabalho da Administração de Sistemas (AdmSist)

Responsabilidades: Responsáveis pela instalação, configuração e manutenção dos sistemas, no entanto, com acesso controlado às configurações relacionadas com a segurança.

Descrição de Tarefas:

- Gestão do ambiente de produção

- Instalação, configuração e manutenção dos sistemas e rede tendo acesso controlado às configurações relacionadas com os componentes aplicacionais
- Gestão do desempenho dos sistemas que suportam a atividade da GTS, de modo a garantir que a infraestrutura esteja sempre disponível e operacional, previsão das necessidades futuras que decorrem da atividade da GTS e os seus custos.
- Gestão dos incidentes e avarias de *hardware* e *software*
- Reposição do sistema através das cópias de segurança, quando necessário
- Execução e manutenção de documentação (procedimentos) pertinentes à execução das suas funções
- Guarda dos artefactos sob a sua custódia

14.2.3. Grupo de Trabalho de Operação de Sistemas (OpSist)

Responsabilidades: Responsáveis pela operação de rotina dos sistemas de confiança, estando autorizados a realizar as cópias de segurança e sua recuperação.

Descrição de Tarefas:

- Operação diária dos sistemas
- Realização de operações de rotina
- Realização de cópias de segurança
- Guarda dos artefactos sob a sua custódia

14.2.4. Grupo de Trabalho de Administração de Registo (AdmReg)

Responsabilidades: Responsáveis pela aprovação da emissão e revogação de certificados digitais (certificados de assinatura qualificada, selos eletrónicos, certificados para autenticação de sítios Web, e selos temporais).

Descrição de Tarefas:

- Emissão/revogação dos certificados
- Submissão dos *Certificate Signing Request* (CSR) para a execução dos processos de registo
- Criação ou atualização das entidades requerentes de serviços de certificação

- Validação da documentação a ser entregue pelo titular para emissão/revogação de certificados
- Notificação dos titulares quando necessário
- Guarda dos artefactos sob a sua custódia

14.2.5. Grupo de Trabalho de Auditoria (Auditor)

Responsabilidades: Responsáveis pela análise interna da conformidade com as normas nacionais e europeias aplicáveis à atividade da GTS enquanto prestadora de serviços qualificados, estando autorizados a ver e monitorizar os arquivos de atividade dos sistemas de confiança.

Descrição de Tarefas:

- Registo e monitorização de todas as operações sensíveis do sistema
- Registo de todos os procedimentos passíveis de auditoria
- Verificação periódica da conformidade com os processos, políticas e procedimentos em vigor no âmbito da atividade de prestadora de serviços qualificados
- Guarda dos artefactos sob a sua custódia
- Apresentação de sugestões de melhoria

14.2.6. Grupo de Trabalho de Gestão (Gestão)

Responsabilidades: Responsáveis por assegurar os meios técnicos, financeiros e humanos para o correto funcionamento da GTS enquanto prestadora de serviços qualificados.

Descrição de Tarefas:

- Nomeação dos membros dos restantes Grupos de Trabalho
- Revisão e aprovação das Políticas e Declaração de Práticas da GTS
- Guarda dos artefactos sob a sua custódia

14.2.7. Número de pessoas exigidas por grupo

Cada grupo deverá ter pelo menos 2 pessoas de modo a garantir a redundância dos recursos.

14.2.8. Segregação de funções

Para cada tarefa serão necessárias 2 pessoas de modo que, a composição dos grupos de trabalho deve respeitar os princípios de privilégio mínimo e segregação de funções.

Deste modo, a tabela a seguir apresenta as incompatibilidades entre os diferentes grupos existentes na GTS, de modo a evitar quaisquer conflitos de interesse.

Grupo de Trabalho	Incompatível com				
	(a)	(b)	(c)	(d)	(e)
(a) Administração de Segurança		x	x	x	x
(b) Administração de Sistemas	X				x
(c) Administração de Registo	X				x
(d) Operação de Sistemas	X				x
(e) Auditoria	X	x	x	x	

14.3. Medidas de segurança de Pessoal

14.3.1. Requisitos relativos às qualificações, experiências, antecedentes e credenciação

Todos os membros que integrem um dos grupos de trabalho da GTS devem cumprir os seguintes requisitos:

- Apresentar provas da suficiente qualificação e experiência para o desempenho da respetiva função
- Garantir confidencialidade relativamente a informação sensível da GTS ou dados de identificação dos titulares
- Garantir que não desempenham funções que possam causar conflito com as suas responsabilidades nas atividades da GTS
- Garantir o conhecimento dos termos e condições para o desempenho da respetiva função
- Ter recebido a documentação necessária para o desempenho da respetiva função
- Ter recebido formação e treino adequado para o desempenho da respetiva função
- Ter sido nomeado formalmente para a função a desempenhar.

14.3.2. Procedimento de verificação de antecedentes

A verificação de antecedentes decorre do processo de credenciação dos indivíduos nomeados para exercer cargos em qualquer um dos Grupos de Trabalho e inclui a verificação da identidade, bem como das referências indicadas no curriculum vitae.

14.3.3. Requisitos de formação e treino

Os membros dos Grupos de Trabalho têm acesso a formação e treino adequado de modo a realizarem as suas tarefas de modo satisfatório e de forma competente, estando adicionalmente sujeitos a um plano que engloba os tópicos seguintes:

- Aspetos legais relativos à prestação de serviços de certificação
- Certificação digital e Infraestruturas de Chave Pública Conceitos gerais sobre segurança da informação
- Formação específica para o Grupo de Trabalho em causa
- Funcionamento do software e/ou hardware usado na GTS
- Política de Certificados e Declaração de Práticas de Certificação
- Procedimentos para a continuidade da atividade
- Recuperação face a desastres.

14.3.4. Frequência e requisitos para ações de reciclagem

Sempre que ocorra qualquer alteração tecnológica, introdução de novas ferramentas ou modificação de procedimentos existentes, deverá desencadear-se um processo de formação adequado para todos os Grupos de Trabalho. Devem ainda ser realizadas sessões formativas aos elementos das Entidades Certificadoras sempre que ocorram alterações às Políticas de Certificação ou na Declaração de Práticas de Certificação da GTS.

Tais factos devem ser tidos em linha de conta de modo a garantir o nível pretendido de conhecimentos para a execução satisfatória das responsabilidades que compete aos diferentes Grupos de Trabalho.

14.3.5. Frequência e sequência da rotação de funções

Nada a assinalar.

14.3.6. Sanções para ações não autorizadas

Todas as ações não autorizadas e que desrespeitem a Declaração de Práticas de Certificação da GTS e as Políticas de Certificados deverão ser alvo de medidas disciplinares adequadas, quer tenham sido realizadas de forma deliberada ou sejam ocasionadas por negligência.

Poderão ainda, de acordo com a gravidade da infração cometida, ser aplicadas sanções previstas na lei.

14.3.7. Requisitos para prestadores de serviços

O acesso à Zona de Alta Segurança por consultores ou prestadores de serviços independentes exige a supervisão contínua pelos membros dos grupos de trabalho, bem como o registo no livro de presenças existente para o efeito.

14.3.8. Documentação fornecida ao pessoal

Deverá ser disponibilizada aos membros dos Grupos de Trabalho a informação e documentação necessária relativamente às Políticas de Certificados, à Declaração de Práticas de Certificação da GTS, à documentação com a descrição das responsabilidades, obrigações e tarefas dependendo da função e ainda documentação técnica acerca do software e hardware utilizado na Entidade Certificadora da GTS.

14.4. Procedimentos de Auditoria de Segurança

14.4.1. Tipo de eventos registados

Deverão ser registados todo o tipo de eventos significativos, capazes de ser auditáveis, em especial os seguintes:

- Cópias de segurança, restauro ou arquivamento de dados;
- Dispositivos físicos de segurança de entrada/saída dos vários níveis de segurança.
- Manutenções ao sistema;
- Modificações ou atualizações relativamente a software e hardware;
- Mudança de pessoal;
- Ligar e desligar aplicações ou sistemas que intervenham na atividade de certificação;
- Operações realizadas por membros dos Grupos de Trabalho;
- Tentativas, com ou sem sucesso, de acesso a recursos sensíveis da Entidade Certificadora da GTS;
- Tentativas, com ou sem sucesso, de alteração dos parâmetros de segurança;
- Tentativas, com ou sem sucesso, de criar, modificar ou apagar contas do sistema;
- Tentativas, com ou sem sucesso, de início e fim de sessão;
- Tentativas, com ou sem sucesso, de operações relativas a pedido, emissão, renovação, modificação, revogação de chaves e certificados;
- Tentativas, com ou sem sucesso, de gerar, emitir ou atualizar LCR;
- Tentativas, com ou sem sucesso, de criar, modificar ou apagar informação dos titulares dos certificados;
- Tentativas, com ou sem sucesso, de acesso às Zonas de Alta Segurança da EC GTS.

O registo dos eventos, efetuado quer por meios automáticos ou manuais, deverá conter, no mínimo, informações tais como a data e hora do evento, a categoria e descrição do mesmo, o número de série do evento, bem como a identificação do agente que o terá originado.

14.4.2. Frequência da auditoria de registos

A auditoria dos registos é realizada mensalmente ou sempre que exista ocorrência de eventos que possam ser considerados suspeitos ou que possam comprometer, de alguma forma, a atividade em questão. Todos esses eventos deverão ficar registados num relatório sumário, passível de ser analisado, bem como as decisões e ações tomadas em resposta a estes.

14.4.3. Período de retenção dos registos de auditoria

Os registos de auditoria são mantidos nos sistemas por um período de pelo menos 1 mês após o seu processamento. Após esse período, deverão ser arquivados tal como definido na seção 14.5.1 do presente.

14.4.4. Proteção dos registos de auditoria

Os registos de auditoria encontram-se protegidos contra as tentativas de acessos, alteração, manipulação ou destruição não-autorizadas.

Por norma, os registos eletrónicos estão protegidos com recurso a técnicas criptográficas de modo a que ninguém, à exceção das próprias aplicações de visualização de registos, com o controlo de acessos adequado, possa aceder aos mesmos.

Os registos manuais são armazenados em locais que cumpram os requisitos definidos para o efeito, dentro de instalações seguras da EC GTS. Este tipo de registos de auditoria é considerado informação sensível.

14.4.5. Procedimentos para a cópia de segurança dos registos

São realizadas cópias de segurança dos registos de auditoria de forma regular.

14.4.6. Sistema de recolha de registos (Interno / Externo)

Os registos são recolhidos e tratados centralmente.

14.4.7. Notificação de agentes causadores de eventos

Os eventos passíveis de serem auditáveis são registados nos sistemas internos da GTS, sendo estes armazenados de forma segura. Não está contemplada qualquer notificação ao agente causador do evento.

14.4.8. Avaliação de vulnerabilidades

Ainda que não ocorram alterações significativas no ambiente global da Entidade Certificadora da GTS, deverão ainda assim ser efetuadas avaliações de vulnerabilidades, tendo em vista minimizar ou eliminar potenciais tentativas de quebras de segurança no sistema. O resultado das avaliações deve ser reportado aos responsáveis pela matéria, para que estes a possam rever e aprovar, caso se justifique, um plano de implementação e correção das vulnerabilidades detetadas, todos registos de eventos auditáveis são regularmente analisados.

14.5. Arquivo de Registos

14.5.1. Tipo de dados arquivados

A EC GTS irá arquivar, no mínimo, os seguintes tipos de dados:

- Os registos de auditoria especificados no ponto 14.4.1 do presente documento;
- As cópias de segurança dos sistemas que compõem a infraestrutura da EC;
- Documentação relativa ao ciclo de vida dos certificados.
- Chaves para efeitos de confidencialidade (quando aplicável);
- Contratos estabelecidos entre a EC e outras entidades.

14.5.2. Período de retenção em arquivo

O tempo de retenção dos dados sujeitos a arquivo está definido de acordo com a legislação nacional, por um período nunca inferior a 7 anos.

14.5.3. Proteção dos arquivos

O arquivo encontra-se protegido de acordo com o que está igualmente previsto para a proteção dos registos de auditoria. Mais se acrescenta que o arquivo se encontra protegido de modo a que apenas os membros autorizados dos Grupos de Trabalho possam consultar e aceder ao mesmo.

14.5.4. Procedimentos para as cópias de segurança do arquivo

De acordo com o disposto no ponto 14.4.5, relativamente aos procedimentos para a cópia de segurança dos registos.

14.5.5. Requisitos para validação cronológica dos registos

Os sistemas de informação utilizados pela EC GTS devem garantir o registo da data e hora do momento, tendo por base uma fonte de tempo segura.

14.5.6. Sistema de recolha de dados de arquivo (Interno / Externo)

De acordo com o disposto no ponto 14.4.6.

14.5.7. Procedimentos de recuperação e verificação de informação arquivada

Só os membros devidamente autorizados dos Grupos de Trabalho têm acesso aos arquivos para a verificação da integridade da informação, de modo a garantir que os mesmos se encontram em bom estado e que podem ser recuperados.

14.6. Comprometimento e Recuperação em Caso de Desastre

14.6.1. Procedimentos em caso de incidente ou comprometimento

Em caso de incidente de segurança grave ou comprometimento da EC GTS, devem ser tomados os procedimentos seguintes:

- Notificação, sem demora indevida, mas sempre no prazo de 24 horas após ter tomado conhecimento do ocorrido, a entidade supervisora e, se necessário, outras entidades, como a entidade nacional competente em matéria de segurança da informação ou a autoridade responsável pela proteção de dados, de todas as violações da segurança ou perdas de integridade que tenham um impacto significativo sobre o serviço de confiança prestado ou sobre os dados pessoais por ele conservados.

- Se a violação da segurança ou perda de integridade constatada for suscetível de prejudicar a pessoa singular ou coletiva a quem o serviço de confiança tiver sido prestado, será notificada também sem demora indevida a referida pessoa singular ou coletiva da violação da segurança ou da perda de integridade.

- Adicionalmente, e dependendo do tipo de incidente, a EC afetada poderá ser desligada.

Se necessário, em particular se a violação da segurança ou a perda de integridade disserem respeito a dois ou mais Estados-Membros, a entidade supervisora notificada informa do facto as entidades supervisoras dos outros Estados-Membros em causa e a ENISA.

A entidade supervisora notificada informa o público ou exige que o prestador do serviço de confiança o faça, se considerar que a divulgação da violação da segurança ou perda de integridade é do interesse público.

14.6.2. Comprometimento do Algoritmo

Se algum dos algoritmos, ou parâmetros associados, utilizados pela EC GTS ou seus titulares se tornarem insuficientes para o fim a que se destinam, a EC GTS deve:

- Informar todos os titulares e outras entidades com as quais a EC GTS tenha acordos ou outra forma de relações estabelecidas. Adicionalmente, esta informação deve ser disponibilizada para outras entidades dependentes;

Agendar a revogação de qualquer certificado afetado.

14.6.3. Corrupção dos recursos informáticos, do software e/ou dos dados

Caso os recursos de hardware, software e/ou dados tenham sido alterados ou exista a suspeita de que estes tenham sido corrompidos, deverá iniciar-se um processo de gestão de incidentes tendo

em vista o restabelecimento das condições seguras com inclusão de novos componentes de eficácia credível.

A GTS suspenderá os seus serviços e notificará todas as Entidades envolvidas caso se verifique que esta situação tenha afetado os certificados emitidos, incluindo a notificação dos titulares dos mesmos.

14.6.4. Capacidade para continuidade da atividade

A GTS dispõe de um plano de continuidade da atividade, onde estão descritos todos os procedimentos a acionar em caso de desastre onde haja perda ou corrupção de dados, software e equipamentos.

O Plano de Continuidade deverá garantir que os serviços indicados como críticos pela sua necessidade de disponibilidade estão disponíveis no Local Alternativo e que os dados da EC GTS necessários para retomar as operações são copiados e armazenados em locais seguros e adequados para permitir retomar devidamente as operações da EC GTS em caso de incidentes/desastres.

As cópias de segurança de informações e software essenciais são realizadas regularmente. Devem ser fornecidas instalações de apoio adequadas para garantir que todas as informações e software essenciais possam ser recuperados após um desastre ou falha nos meios de comunicação (media). Os mecanismos de salvaguardas devem ser testados regularmente para garantir que respondem aos requisitos dos planos de continuidade do negócio.

14.6.5. Procedimentos em caso de Extinção da Entidade de Certificação ou Entidade de Registo

A GTS deve em caso de cessação de atividades, atempadamente proceder às ações seguintes:

a) Informar a Entidade Supervisora (Gabinete Nacional de Segurança);

b) Informar todos os titulares dos certificados a partir de uma notificação explanatória com antecedência à cessação formal das atividades da EC GTS;

c) Revogar todos os certificados;

d) Garantir a transferência (para retenção por outra organização) de toda a informação relativa à atividade da EC, nomeadamente, chave da EC, certificados, documentação em arquivos (interno ou externo), repositórios e arquivos de registo de eventos;

e) Proceder à destruição definitiva de toda a informação classificada ou garantir a transferência (para retenção por outra organização) de toda a informação relativa à atividade da EC GTS, nomeadamente, chave da EC, certificados, documentação em arquivos (interno ou externo), repositórios e arquivos de registo de eventos.

Em caso se procedam alterações do organismo/estrutura responsável de gestão da atividade da EC GTS, esta deve informar de tal facto às entidades listadas nas alíneas anteriores.

15. Controlos de Segurança Técnicos

15.1. Geração e Instalação de Pares de Chaves

A geração dos pares de chaves da EC GTS é processada de acordo com os requisitos e algoritmos definidos nesta declaração, através de um procedimento formal datado, realizado e assinado por elementos autorizados dos Grupos de Trabalho da Administração de Segurança e de Auditoria.

O processo de geração das chaves é, obrigatoriamente, efetuado diretamente num módulo criptográfico em hardware (HSM). O módulo criptográfico cumpre os requisitos FIPS 140-2 nível 3, gerando uma chave não sequencial. Estes certificados são assinados pela EC GTS.

A EC GTS funciona em modo *online*.

No que respeita à dimensão das chaves, foram seguidas as recomendações da norma ETSI TS 119 312 – Electronic Signatures and Infrastructures – Cryptographic Suites. A dimensão definida para as chaves é a seguinte:

- 4096 bits RSA para a chave das entidades certificadoras da GTS.
- 2048 bits RSA para chaves associadas aos restantes certificados que sejam emitidos pela GTS com algoritmo de assinatura sha256RSA.

A geração das chaves da EC GTS deverá ser feita de acordo com o estipulado no PKCS#11.

15.2. Proteção da Chave Privada e Características do Modulo Criptográfico

A EC GTS utiliza módulos criptográficos (HSM) para as operações que dizem respeito à geração, armazenamento e assinatura.

Os módulos criptográficos estão em conformidade com o Common Criteria v2.3, FIPS 140-2 nível 3 (para o módulo criptográfico da ROOT CA GTS).

A segurança do módulo criptográfico da Entidade de Certificação da GTS é garantida durante o seu ciclo de vida, garantindo os seguintes:

- A instalação e ativação das chaves privadas no módulo criptográfico é efetuada por elementos de Grupos de Trabalho bem identificados (secção 14.2 Controlos dos Processos e 14.3 Medidas de Segurança de Pessoal);
- As chaves privadas de assinatura guardadas no módulo criptográfico são apagadas no final do seu ciclo de vida.
- O módulo criptográfico não foi adulterado durante o seu transporte;O módulo criptográfico não é adulterado enquanto permanece nas instalações seguras da GTS;
- O módulo criptográfico tem um funcionamento correto;

A EC GTS efetua a retenção da sua chave privada e das chaves privadas de todos os seus clientes através de um HSM guardado em ambiente seguro.

As chaves privadas da EC GTS:

- Têm pelo menos uma cópia de segurança, com o mesmo nível de segurança que a chave original e são alvo de cópias de segurança
- São arquivadas internamente em ambientes seguros por 20 anos.
- São geradas e armazenadas em HSM não sendo possível a transferência das mesmas para outros meios ou dispositivos.
- São armazenadas de forma cifrada em HSM.

A chave privada deverá ser ativada quando o sistema quando o sistema/aplicação da ROOT CA é ligado. Esta ativação só será efetivada quando previamente tiver sido feita a autenticação no módulo criptográfico pelos indivíduos indicados para o efeito, sendo obrigatória a utilização de autenticação por quórum k em N onde k = 2. Isso é, é necessário k utilizadores em N para efetuar uma operação administrativa nos HSM (incluindo a ativação da chave privada). A chave privada permanecerá ativa até que o processo de desativação seja executado.

As várias chaves privadas da EC GTS deverão ser destruídas sempre que deixem de ser necessárias. De uma forma geral, a destruição de chaves deve ser precedida sempre pela revogação do certificado, no caso de estar em vigor, ou caso tenha sido atingido o fim da sua data de validade. Nesse sentido, as chaves deverão ser apagadas/destruídas através de um método formal auditável, de modo a que não seja possível a sua posterior reconstrução. De igual forma, as respetivas cópias de segurança deverão também ser alvo de destruição.

15.3. Outros Aspetos da Gestão do Par de Chaves

A EC GTS efetua o arquivo das suas chaves e das chaves por si emitidas (para efeitos de assinatura digital), permanecendo armazenadas após a expiração dos certificados correspondentes para verificação de assinaturas geradas durante seu período de validade.

O período de utilização das chaves é determinado pelo período de validade do certificado, pelo que após expiração do certificado as chaves deixam de poder ser utilizadas, dando origem à cessação permanente da sua operacionalidade e da utilização que lhes foi destinada.

A validade dos diversos tipos de certificados e período em que os mesmos devem ser renovados, é o seguinte:

- O certificado da EC GTS tem uma validade mínima de 6 anos;
- Um certificado SSL/TLS emitido pela Entidade de Certificação da GTS tem uma validade mínima de 1 ano, e máxima de 3 anos.

- Um certificado de autenticação para os Administradores de Registo da Entidade de Certificação da GTS têm uma validade mínima de 1 ano e máxima de 3 anos.

- Um certificado para um Serviço da EC GTS têm uma validade mínima de 1 ano e máxima de 10 anos.

A EC GTS não emite certificados com validade superior ao seu próprio certificado.

15.4. Dados de Ativação

A geração e instalação dos dados de ativação para a chave privada da EC GTS é feita por pessoal autorizado em ambiente seguro através de um setup inicial do HSM, que exige controlo simultâneo por dois membros dos grupos de trabalho.

Os dados de ativação da chave privada são guardados em ambientes seguros (secção Proteção da Chave Privada e Características do Modulo Criptográfico).

A transmissão dos dados de ativação das chaves privadas para outros HSM é feita, apenas e só quando necessário, de modo a garantir a sua proteção e disponibilidade.

Os dados de ativação são destruídos assim que a chave privada associada for igualmente destruída.

15.5. Controlos de Segurança Informática

A EC GTS tem um funcionamento *online*, cujos pedidos de emissão de certificados são efetuados a partir de uma plataforma web disponível em https://www.globaltrustedsign.com. O acesso aos servidores da GTS é restrito apenas a membros autorizados.

Controlos contra acessos não autorizados:

- Firewalls que dividem a infraestrutura física em duas zonas, uma Zona de Acesso Externo (ZAE) e uma Zona de Alta Segurança (ZAS);

- O uso de canais seguros no acesso às plataformas web públicas da GTS na ZAE nos respetivos portos/protocolos (HTTPS);

- O uso de canais seguros entre as Serviços e Servidores nas ZAS nos respetivos portos/protocolos (HTTPS);

- Todos os portos/protocolos não utilizados estão bloqueados pelas Firewalls.

Controlos contra modificações:

- Toda a comunicação entre componentes da infraestrutura da GTS é feita sobre o protocolo de HTTPS, protegendo deste modo a informação em trânsito.

- A plataforma web faz uso do protocolo HTTPS para proteção da informação em trânsito.

- A plataforma web só pode ser acedida pós autenticação dos utilizadores.

15.6. Ciclo de Vida dos Controlos de Segurança

Todo o desenvolvimento, configuração e alteração do software/hardware associados à infraestrutura de chave pública são executadas e auditadas por membros autorizados da GTS.

A GTS possui mecanismos para controlar e monitorizar as configurações dos sistemas da EC GTS deste a sua primeira ativação até à eventual cessação de atividades, nomeadamente:

- Um sistema de monitorização na ZAS, que monitoriza entre outros aspetos, o espaço em disco dos servidores, a memória utilizada;
- Uma plataforma de ticketing para gestão de incidentes e agregação de eventos, inclusive eventos enviados pelo sistema de monitorização.

Todas as operações de atualização e manutenção são executadas por membros autorizados de acordo com os procedimentos adequados para o efeito.

15.7. Controlos de Segurança da Rede

A infraestrutura da GTS dispõe de sistemas de *firewall* (secção 15.5 Controlos de Segurança Informática). Todos os sistemas da EC GTS estão na Zona e de Alta Segurança (ZAS). Através dos controlos implementados, é possível garantir a identificação, autenticação e administração dos acessos.

15.8. Validação Cronológica

A informação relacionada com a ROOT CA GTS é registada com a data e hora da criação.

Toda a infraestrutura é sincronizada temporalmente por relógio atómico interno, e adicionalmente por duas fontes UTC alternativas:

- Real Instituto y Observatorio de la Armada, San Fernando, Spain - hora.roa.es
- Observatoire de Paris (LNE-SYRTE), Paris, France - ntp-p1.obspm.fr

16. Perfil de Certificado e de Listas de Revogação de Certificados

16.1. Perfil de Certificado

A emissão de certificados segue o perfil de certificados recomendado pela ITU-T X.509 versão 3.

O armazenamento das chaves envolvidas em todos os processos de assinatura ou geração de certificados são guardados num Dispositivo Seguro de Hardware (HSM) certificado e que cumpre os requisitos definidos na legislação nacional e europeia.

O perfil do certificado da EC GTS está de acordo com o conjunto de standards:

- Regulamento (UE) N.º 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE

- ETSI EN 319 401 – General Policy Requirements for Trust Service Providers, e os standards relacionados com os serviços qualificados de confiança
- Outra legislação nacional e europeia relacionada com a atividade de prestação de serviços de confiança qualificados.

Informação detalhada sobre os perfis dos Certificados da EC GTS pode ser consultada em:

- https://pki.globaltrustedsign.com/index.html

16.2. Perfil de Listas de Revogação de Certificados

As LRC emitidas contêm os campos básicos e conteúdos específicos na tabela seguinte:

Campo	Valor
Versão	V2
Algoritmo de Assinatura	O algoritmo utilizado pela EC para assinar o certificado é sha256WithRSAEncryption
Emissor	DN da entidade certificadora emissora da LCR
Data Efetiva	A indicação de quando a LCR foi gerada.
Próxima atualização	A indicação de quando será gerada nova LCR.
Certificados Revogados	Lista dos certificados revogados que fornece informação do estado dos certificados no que diz respeito, respetivamente, ao número de série do certificado revogado, a data em que foi revogado e o motivo da sua revogação.

Informação mais detalhada sobre os perfis das LRC e OCSP pode ser consultada em:

- Lista de Revogação de Certificados (LRC) da EC GTS
  https://pki.globaltrustedsign.com/index.html
- Lista de Revogação de Certificados (LRC) da EC GTS
  https://pki02.globaltrustedsign.com/index.html
- O perfil dos certificados OCSP pode ser consultado em:
  http://ocsp.globaltrustedsign.com

17. Auditoria e Avaliação de Conformidade

A GTS irá efetuar auditorias e avaliações de conformidade regulares para assegurar a conformidade da Entidades Certificadoras constituintes da sua hierarquia de confiança de acordo com legislação nacional bem como com as normas internacionais aplicáveis.

Nota: A GTS, ou os seus representantes legais, podem delegar a realização destas auditorias, avaliações ou investigações a entidades externas de auditoria devidamente especializadas e acreditadas para o efeito.

17.1. Frequência ou motivo da auditoria

Na EC GTS, as auditorias de conformidade serão realizadas regularmente de acordo com a legislação aplicável por uma entidade externa registada e reconhecida para o efeito, tomando como base as normas existentes sendo os seus resultados comunicados à entidade supervisora. Adicionalmente a realização da auditoria anual por parte de uma entidade externa, a EC GTS realiza mensalmente auditorias internas.

17.2. Identidade e qualificações do Organismo de Avaliação da Conformidade

O Organismo de avaliação da conformidade (Conformity Assessment Body – CAB) é o organismo definido no artigo 2.º, n.º 13, do Regulamento (CE) n.º 765/2008, que é acreditado nos termos do mesmo regulamento como sendo competente para realizar a avaliação da conformidade de prestadores qualificados de serviços de confiança e dos serviços de confiança prestados por estes.

17.3. Relação entre o Organismo de Avaliação da Conformidade e a EC GTS

O organismo de avaliação da conformidade e membros da sua equipa são independentes, não atuando de forma parcial ou discriminatória em relação à entidade que é submetida à auditoria.

Na Relação entre o auditor e a entidade submetida a auditoria, deve estar garantido inexistência de qualquer vínculo contratual.

O Auditor e a parte auditada (Entidade Certificadora) não devem ter nenhuma relação, atual ou prevista, financeira, legal ou de qualquer outro género que possa originar um conflito de interesses.

O cumprimento do estabelecido na legislação em vigor sobre a proteção de dados pessoais, deve ser tida em conta por parte do auditor, na medida em que o auditor poderá aceder a dados pessoais dos ficheiros dos titulares da EC GTS.

17.4. Âmbito da auditoria

Uma auditoria de segurança é efetuada com base nos requisitos definidos na presente DPC e em conformidade com a legislação nacional aplicável. Tem por objetivo determinar a conformidade dos serviços da EC GTS com esta Declaração de Práticas e com as Políticas de Certificados definidas.

Deve também determinar a correta adequação em relação a diversos documentos, nomeadamente a política de segurança, segurança física, avaliação tecnológica, gestão dos serviços da EC, seleção de pessoal, declarações de práticas de certificação e políticas de certificados em vigor, contratos e política de privacidade.

Pode ser efetuada de forma completa ou parcial, e pode incidir sobre qualquer tipo de documentos/processos.

17.5. Procedimentos após uma auditoria com irregularidades identificadas

Quando são detetadas irregularidades numa auditoria, a CAB deve proceder da seguinte forma:

a) Documentar todas as irregularidades encontradas durante a auditoria;

b) No final do processo de auditoria, reunir com os responsáveis da entidade submetida a auditoria e apresentar de forma sucinta o relatório de primeiras impressões (RPI);

c) Elaborar o relatório de auditoria de acordo com as regras e práticas estabelecidas pela Entidade Supervisora;

d) Submeter o relatório de auditoria à Entidade auditada;

e) A entidade submetida à auditoria deve enviar um relatório de correção de irregularidades (RCI) para a Entidade Supervisora, descrevendo as ações, metodologia e tempo necessário para a correção das irregularidades identificadas;

f) A Entidade Supervisora após a análise do relatório submetido, consoante o nível de gravidade/severidade das irregularidades, tomará uma das três opções seguintes:

   a. Aceitar os termos, permitindo que a atividade seja desenvolvida até à próxima inspeção;

   b. Permitir que a entidade continue em atividade por um período máximo de 90 dias para a correção das irregularidades;

   c. Revogação imediata das atividades.

17.6. Comunicação de resultados

Os resultados de todo o processo serão comunicados aos auditores responsáveis e à GTS.

18. Outras Situações e Assuntos Legais

Estabelecem-se alguns aspetos legais e de negócio que importa salientar de seguida:

- Poderão ser cobradas taxas pelos processos de emissão, e/ou renovação de certificados;

- Poderão ser cobradas taxas pelos serviços de validação cronológica;
- Não serão cobradas taxas pela disponibilização dos certificados em repositório;

- O acesso a informação sobre o estado ou lista de revogação de certificados (LRC) é livre e gratuita, não se podendo aplicar qualquer taxa;
- Não estão previstos reembolsos aplicáveis à prestação de serviços de revogação de certificados.

18.1. Responsabilidade Financeira

18.1.1. Seguro de cobertura

A GTS dispõe do seguro obrigatório de responsabilidade civil, conforme artigo 16.º do Decreto-Lei n.º 62/2003, de 3 de abril.

18.1.2. Outros recursos

Nada a assinalar.

18.1.3. Seguro ou garantia de cobertura para utilizadores

A GTS dispõe do seguro obrigatório de responsabilidade civil, conforme artigo 16.º do Decreto-Lei n.º 62/2003, de 3 de abril.

18.2. Confidencialidade da Informação Processada

O pedido de inclusão no certificado de dados pessoais da pessoa singular a constar como seu titular terá de ser expressamente autorizado pela própria.

Considera-se informação confidencial:

- As chaves privadas das Entidades Certificadoras;
- As chaves privadas dos titulares dos certificados;
- Toda a informação relativa aos parâmetros de segurança, controlo e procedimentos de auditoria;
- Toda a informação de carácter pessoal proporcionada à EC GTS durante o processo de registo dos subscritores de certificados, salvo se houver autorização explícita para a sua divulgação;
- Planos de continuidade de negócio e recuperação;
- Registos de transações, incluindo os registos completos e os registos de auditoria das transações;
- Dados dos membros dos grupos de trabalho da EC GTS.

Considera-se informação de acesso público:

- Declarações de Práticas de Certificação;
- Políticas de Certificados;
- Listas de Revogação de Certificados (LRCs);
- Toda a informação classificada como "pública".

A EC GTS permite o acesso a informação não confidencial, sem prejuízo do que se venha a estabelecer nas DPC, no domínio dos controlos de segurança necessários para proteger a autenticidade e integridade da mesma.

18.3. Privacidade dos Dados Pessoais

Informação privada é toda a informação fornecida pelo titular do certificado que não esteja publicamente disponível. Informação considerada não-privada é toda a informação tornada pública a partir de certificados, não é considerada privada.

A responsabilidade de proteção da informação privada, assim como os procedimentos para notificação e consentimento para utilização da informação privada estão de acordo com a legislação portuguesa, nomeadamente com o regulamento geral de proteção de dados (regulamento 2016/679). Os dados fornecidos apenas serão disponibilizados publicamente para extração se tiver sido obtido o consentimento da pessoa a quem os dados digam respeito.

As práticas da EC GTS garantem a proteção da confidencialidade e integridade dos dados de registo, especialmente quando transmitida entre a EC GTS e os subscritores e titulares, bem como durante a comunicação entre os componentes distribuídos dos sistemas da EC GTS.

No âmbito dos serviços prestados, é necessário manter evidências digitais por questões de conformidade com a legislação em vigor e aplicável à EC GTS. Estas evidências são mantidas de modo a garantir a sua recolha, transmissão e armazenamento seguros.

18.4. Direitos de Propriedade Intelectual

Todos os direitos de propriedade intelectual, incluindo os que se referem a certificados e LCR emitidos, OID, DPC, PC, bem como qualquer outro documento relacionado, são propriedade da EC GTS.

As chaves privadas e as chaves públicas são propriedade do titular, independentemente do meio físico que se empregue para o seu armazenamento.

O titular conserva sempre o direito sobre as suas marcas, produtos ou nome comercial contido no certificado.

18.5. Representações e Garantias

É obrigação da EC GTS cumprir as diretivas seguintes:

- Realizar as suas operações de acordo com esta Declaração de Práticas;
- Declarar de forma clara todas as suas Práticas de Certificação no documento apropriado;
- Cumprir com as especificações contidas na legislação sobre Proteção de Dados Pessoais;
- Proteger, em caso de existirem, as suas chaves privadas e as que estejam sob sua custódia;
- Emitir certificados de acordo com o standard X.509;
- Emitir certificados que estejam conformes com a informação conhecida no momento de sua emissão e livres de erros de input de dados;
- Garantir a confidencialidade no processo da geração dos dados da criação da assinatura e a sua entrega por um procedimento seguro ao titular;
- Utilizar sistemas e produtos fiáveis que estejam protegidos contra toda a alteração e que garantam a segurança técnica e criptográfica dos processos de certificação;
- Utilizar sistemas fiáveis para armazenar certificados reconhecidos, que permitam comprovar a sua autenticidade e impedir pessoas não autorizadas altere os dados;
- Arquivar sem alteração os certificados emitidos;
- Garantir que pode determinar, com precisão da data e hora, em que emitiu, ou revogou, um certificado;
- Empregar pessoal com qualificações, conhecimento e experiências necessárias para a prestação de serviços de certificação;
- Revogar os certificados nos termos previstos no presente documento, e atualizar a lista de certificados revogados na LCR, com a frequência estipulada na presente DPC.
- Publicar a sua DPC e as Políticas aplicáveis no seu repositório garantindo o acesso às versões atuais assim como as versões anteriores;
- Notificar, com a máxima brevidade possível, por meio de correio eletrónico, os titulares dos certificados nos casos em que a EC GTS proceda à revogação dos mesmos, indicando o motivo que originou a situação;
- Colaborar com as auditorias externas exigidas pela Entidade Supervisora;

- Operar em conformidade com as políticas, normas e legislação que sejam aplicáveis;

- Garantir a disponibilidade da LCR de acordo com as disposições do presente documento, bem como a disponibilidade do serviço de OCSP;

- Em caso de cessação de atividades deverá comunicar esse facto com uma antecedência mínima de três meses à Entidade Supervisora, assim como todos os titulares de certificados emitidos pela EC GTS;

- Conservar toda a informação e documentação relativa a um certificado reconhecido e as Declarações de Práticas de Certificação vigentes em cada momento durante o prazo estabelecido no presente documento;

- Disponibilizar os certificados da ROOT CA GTS e EC GTS.

É obrigação dos titulares de certificados emitidos cumprir as diretivas seguintes:

- Limitar e adequar a utilização dos certificados de acordo com a legislação vigente e com as utilizações previstas no presente documento;

- Tomar todos os cuidados e medidas necessárias para garantir a posse da sua chave privada;

- Solicitar de imediato a revogação de um certificado, em caso de ter conhecimento ou suspeita de compromisso da chave privada correspondente à chave pública contida no certificado, de acordo com os procedimentos especificados no presente documento;

- Não utilizar um certificado digital que tenha perdido a sua eficácia, quer por ter sido revogado, ou por ter expirado o período de validade;

- Submeter às Entidades Certificadoras (ou de Registo) a informação que considerem exata e completa em relação aos dados que estas solicitem para realizar o processo de registo. Deve informar a EC de qualquer modificação desta informação;

- Não monitorizar, manipular ou efetuar ações de "engenharia inversa" sobre a implantação técnica (hardware e software) dos serviços de certificação, sem a devida autorização prévia, por escrito, da EC GTS.

É obrigação das partes confiantes dos certificados emitidos pela EC GTS:

- Limitar a fiabilidade dos certificados às utilizações permitidas para os mesmos em conformidade com a legislação vigente e com o presente documento;

- Verificar a validade dos certificados no momento de realizar qualquer operação baseada nos mesmos;

- Assumir a responsabilidade na correta verificação das assinaturas digitais;
- Assumir a responsabilidade na comprovação da validade, revogação dos certificados em que confia;
- Assumir a responsabilidade na correta verificação dos certificados emitidos;
- Ter pleno conhecimento das garantias e responsabilidades aplicáveis na aceitação e uso de certificados em que confia e aceitar sujeitar-se às mesmas;
- Notificar qualquer acontecimento ou situação anómala relativa aos certificados, utilizando os meios que a EC GTS publique no seu espaço Web.

18.6. Renúncia de Garantias

A EC GTS recusa todas as garantias de serviço que não se encontrem vinculadas nas obrigações estabelecidas nesta DPC.

18.7. Limitações às Obrigações

A EC GTS garante os danos ou prejuízos causados aos utilizadores finais e partes confiantes decorrentes da sua atividade, conforme legislação aplicável.

A EC GTS não se responsabiliza por qualquer dano ou prejuízo decorrente utilizações abusivas ou fora do âmbito do contrato estabelecido com os utilizadores e/ou partes confiantes.

A EC GTS não assume qualquer responsabilidade em caso falha dos serviços relacionada com causas de força maior, como desastres naturais, guerra ou outros similares.

18.8. Indeminizações

A EC GTS assumirá a sua responsabilidade no tocante a eventuais indemnizações, de acordo com a legislação aplicável.

18.9. Termo e Cessão da Atividade

Esta DPC entra em vigor desde o momento de sua publicação no repositório da EC GTS e após aprovação, nos termos do presente documento.

Esta DPC estará em vigor enquanto não for revogada expressamente pela emissão de uma nova versão, nos termos do presente documento, ou pela renovação das chaves da ROOT CA GTS ou EC GTS, momento em que, obrigatoriamente, se redigira uma nova versão.

Esta DPC será substituída por uma nova versão, com independência da transcendência das mudanças efetuadas na mesma, de modo que será sempre de aplicação na sua totalidade.

Quando a DPC ficar revogada será retirada do repositório público, garantindo-se que será conservada durante o período definido no presente documento.

As obrigações e restrições que estabelece esta DPC, em referência a auditorias, informação confidencial, obrigações e responsabilidades da EC GTS, nascidas sob a sua vigência, subsistirão após sua substituição ou revogação, por uma nova versão, em tudo o que não se oponha a esta.

18.10. Notificação Individual e Comunicação dos Participantes

Todos os participantes devem utilizar os mecanismos apropriados para a comunicação coletiva, onde se engloba o correio eletrónico assinado digitalmente, correio postal e formulários assinados, entre outros, recorrendo ao meio mais adequando em função da natureza de cada assunto.

18.11. Alterações

As alterações a esta DPC devem ser aprovadas pelo Grupo de Gestão. As alterações devem ser efetuadas através de documentos, contendo as novas alterações à DPC.

No caso em que o Grupo de Gestão julgue que as mudanças à especificação podem afetar à aceitabilidade dos certificados para propósitos específicos, comunicar-se-á aos utilizadores dos certificados correspondentes, que se efetuou uma mudança e que devem consultar a nova DPC no repositório estabelecido. O mecanismo de comunicação será o sítio da internet https://www.globaltrustedsign.com.

Se a EC GTS determinar que a alteração ao identificador (OID) da DPC ou política de certificados é necessária, a alteração deve conter os novos identificadores. De outra forma, as alterações não devem implicar uma mudança no identificador da política de certificados.

18.12. Disposições para Resolução de Conflitos

As reclamações devem ser endereçadas ao Grupo de Gestão da EC GTS, através de carta registada.

Qualquer litígio decorrente da interpretação ou aplicação deste documento regem-se pela lei portuguesa. Para regular esses litígios, as partes elegem o foro judicial da Comarca de Funchal, com exclusão de qualquer outro.

Todas as reclamações entre os utilizadores e a EC GTS poderão ser comunicadas à Entidade Supervisora com a finalidade da resolução de conflitos que possam na eventualidade surgir.

18.13. Legislação Aplicável

A seguinte legislação é aplicável às entidades certificadoras prestadoras de serviços de confiança:

a) Regulamento (UE) N. o 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE

b) Outra legislação nacional e europeia relacionada com a atividade de prestação de serviços de confiança qualificados.

18.14. Conformidade com Legislação em Vigor

O presente documento (DPC) é objeto de aplicação das leis que vigoram em território nacional, bem como das normas e legislações europeias.

18.15. Providências Várias

As partes confiantes assumem, na sua totalidade, o conteúdo da última versão desta DPC.

Em caso, de existirem uma ou mais estipulações do presente documento, que sejam ou tendam a ser inválidas, nulas, ou irreclamáveis em termos jurídicos, deverão ser consideradas como não efetivas. Estas determinações são válidas, apenas e só apenas nos casos em que tais estipulações não sejam consideradas essenciais. É da responsabilidade do Grupo de Gestão avaliar a essencialidade das mesmas.

As práticas adotadas pela EC GTS garantem a independência dos membros dos grupos de confiança e da administração de topo, e a liberdade face a pressões comerciais, financeiras ou outras que possam influenciar a confiança nos serviços por eles prestados.

A EC GTS disponibiliza certificados de teste para os atuais e potenciais utilizadores dos serviços a partir do site https://www.globaltrustedsign.com.

A EC GTS garante as condições para que os seus serviços sejam utilizados por pessoas com deficiência, em conformidade com o regulamento europeu 910/2016.

Anexo A – Acrónimos e Definições

Acrónimos	
C	*Country*
CN	*Common Name*
DN	Nome Distinto *(Distinguished Name)*
DPC	Declaração de Práticas de Certificação
DR	Decreto Regulamentar
EC	Entidade Certificadora
ER	Entidade de Registo
GNS	Gabinete Nacional de Segurança
GTS	*Global Trusted Sign*
HSM	Modulo Criptográfico em Hardware (*Hardware Secure Module*)
LRC	Lista de Revogação de Certificados
O	*Organization*
OU	*Organization Unit*
OID	Identificador de Objeto
PC	Política de Certificado
PKCS	*Public-Key Cryptography Standards*
PKI	Infraestrutura de Chave Pública *(Public Key Infrastructure)*
SSL/TLS	*Secure Sockets Layer / Transport Layer Security*

18.16. Definições

Definições	
Termo	**Definição**
Assinatura Eletrónica	Dados em formato eletrónico que se ligam ou estão logicamente associados a outros dados em formato eletrónico e que sejam utilizados pelo signatário para assinar
Assinatura Eletrónica Avançada	Assinatura eletrónica que obedeça aos requisitos: a) Esteja associada de modo único ao signatário b) Permita identificar o signatário c) Seja criada utilizando dados para a criação de uma assinatura eletrónica que o signatário pode, com um elevado nível de confiança, utilizar sob o seu controlo exclusivo, e d) Esteja ligada aos dados por ela assinados de tal modo que seja detetável qualquer alteração posterior dos dados
Autenticação	Processo eletrónico que permite a identificação eletrónica de uma pessoa singular ou coletiva ou da origem e integridade de um dado em formato eletrónico a confirmar
Certificado	Estrutura de dados assinado eletronicamente por um prestador de serviços de certificação e que vincula ao titular os dados de validação de assinatura que confirma a sua identidade.
Certificado de Assinatura Eletrónica	Atestado eletrónico que associa os dados de validação da assinatura eletrónica a uma pessoa singular e confirma, pelo menos, o seu nome ou pseudónimo
Certificado de Autenticação de Sítio Web	Atestado que torne possível autenticar um sítio web e associe o sítio web à pessoa singular ou coletiva à qual o certificado tenha sido emitido
Certificado de Selo Eletrónico	Atestado eletrónico que associa os dados de validação do selo eletrónico a uma pessoa coletiva e confirma o seu nome
Certificado Qualificado de Assinatura Eletrónica	Certificado de assinatura eletrónica, que seja emitido por um prestador de serviços de confiança e satisfaça os requisitos estabelecidos no anexo I do Regulamento europeu 910/2014
Certificado Qualificado de Autenticação de Sítios Web	Certificado de autenticação de sítios web que seja emitido por um prestador de serviços de confiança e satisfaça os requisitos estabelecidos no anexo I do Regulamento europeu 910/2014
Certificado Qualificado de Selo Eletrónico	Certificado de selo eletrónico emitido por um prestador qualificado de serviços de confiança que satisfaça os requisitos estabelecidos no anexo III do Regulamento europeu 910/2014
Chave Privada	Elemento do par de chaves assimétricas destinado a ser conhecido apenas pelo seu titular, mediante o qual se apõe a assinatura digital no documento eletrónico, ou se decifra um documento eletrónico previamente cifrado com a correspondente chave pública

Definições	
Termo	**Definição**
Chave Pública	Elemento do par de chaves assimétricas destinado a ser divulgado, com o qual se verifica a assinatura digital aposta no documento eletrónico pelo titular do par de chaves assimétricas, ou se cifra um documento eletrónico a transmitir ao titular do mesmo par de chaves
Credenciação	Ato pelo qual é reconhecido a um prestador de serviços que o solicite e que exerça a atividade de entidade certificadora em conformidade com os requisitos definidos no Regulamento europeu 910/2014
Criador de um Selo	Pessoa coletiva que cria um selo eletrónico
Dados de Identificação Pessoal	Conjunto de dados que permita determinar a identidade de uma pessoa singular ou coletiva ou de uma pessoa singular que represente uma pessoa coletiva
Dados de Validação	Dados que são utilizados para validar uma assinatura eletrónica ou um selo eletrónico
Dados para a Criação de um Selo Eletrónico	Conjunto único de dados que seja utilizado pelo criador do selo eletrónico para criar um selo eletrónico
Dados para a Criação de uma Assinatura Eletrónica	Conjunto único de dados que é utilizado pelo signatário para criar uma assinatura eletrónica
Dispositivo de Criação de Assinaturas Eletrónicas	*Software* ou *hardware* configurados, utilizados para criar assinaturas eletrónicas
Dispositivo de Criação de Selos Eletrónicos	*Software* ou *hardware* configurados, utilizados para criar selos eletrónicos
Dispositivo Qualificado de Criação de Assinaturas Eletrónicas	Dispositivo para a criação de assinaturas eletrónicas que cumpra os requisitos estabelecidos no anexo II do Regulamento europeu 910/2014
Dispositivo Qualificado de Criação de Selos Eletrónicos	Dispositivo para a criação de selos eletrónicos que satisfaça *mutatis mutandis* os requisitos estabelecidos no anexo II do Regulamento europeu 910/2014
Documento Eletrónico	Qualquer conteúdo armazenado em formato eletrónico, nomeadamente texto ou gravação sonora, visual ou audiovisual
Endereço Eletrónico	Identificação de um equipamento informático adequado para receber e arquivar documentos eletrónicos.
Entidade Certificadora	Entidade ou pessoa singular ou coletiva credenciada como prestador qualificado de serviços de confiança pela entidade supervisora
Entidade de Registo	Entidade que aprova os Nomes Distintos (DN) das entidades subordinadas e, mediante avaliação do pedido, aceita ou rejeita a solicitação do mesmo
Entidade Supervisora	Entidade competente para a credenciação e fiscalização das entidades certificadoras
Função Hash	Operação que se realiza sobre um conjunto de dados de qualquer tamanho de forma que o resultado obtido é outro conjunto de dados de tamanho fixo independente do tamanho original e que tem a propriedade de estar associado univocamente aos dados inicias e garantir que é impossível obter mensagens distintas que gerem o mesmo resultado ao aplicar esta função.

Definições	
Termo	**Definição**
Hash ou Impressão Digital	Resultado de tamanho fixo que se obtém após a aplicação de uma função hash a uma mensagem e que cumpre a requisito de estar associado univocamente aos dados iniciais
HSM	Módulo de segurança criptográfico empregue para armazenar chaves e realizar operações criptográficas de modo seguro
Identificação Eletrónica	O processo de utilização dos dados de identificação pessoal em formato eletrónico que representam de modo único uma pessoa singular ou coletiva ou uma pessoa singular que represente uma pessoa coletiva
Infraestrutura de Chave Pública	Estrutura de hardware, software, pessoas, processos e políticas que usa a tecnologia de assinatura digital para dar a terceiros de confiança uma associação verificável entre a componente pública de um par de chaves assimétrico e um assinante específico
LCR	Lista de certificados revogados que é criada e assinada pela EC que emitiu os certificados. Um certificado é introduzido na lista quando é revogado (por exemplo, por suspeita de comprometimento da chave). Em determinadas circunstâncias, a EC pode dividir uma LCR num conjunto de LCR mais pequenas
Meio de Identificação Eletrónica	Uma unidade material e/ou imaterial que contenha os dados de identificação pessoal e que seja utilizada para autenticação de um serviço em linha
OID	Identificador alfanumérico/numérico único registado em conformidade com a norma de registo ISO, para fazer referência a um objeto específico ou a uma classe de objetos específica
Organismo de Avaliação da Conformidade	Organismo definido que é acreditado nos termos do regulamento 910/2014 como sendo competente para realizar a avaliação da conformidade de prestadores qualificados de serviços de confiança e dos serviços de confiança qualificados prestados
Organismo Público	Entidade estatal nacional, regional ou local, um organismo de direito público ou uma associação formada por uma ou mais dessas entidades ou por um ou mais organismos de direito público, ou uma entidade privada mandatada por, pelo menos, uma dessas autoridades, organismos ou associações como sendo de interesse público, ao abrigo de tal mandato
Parte Confiante	As partes confiantes ou destinatários são pessoas singulares ou entidades que confiam na validade dos mecanismos e procedimentos utilizados no processo de associação de um selo temporal ao datum, ou seja, confiam na veracidade do selo temporal.
Política de Certificado	Conjunto de regras que indica a aplicabilidade do certificado a uma comunidade específica e/ou classe de aplicação com requisitos de segurança comuns
Prestador de Serviços de Confiança	Pessoa singular ou coletiva que preste um ou mais do que um serviço de confiança quer como prestador qualificado quer como prestador não qualificado de serviços de confiança

Definições	
Termo	**Definição**
Prestador Qualificado de Serviços de Confiança	Prestador de serviços de confiança que preste um ou mais do que um serviço de confiança qualificado e ao qual é concedido o estatuto de qualificado pela entidade supervisora
Produto	*Hardware* ou *software*, ou componentes pertinentes de hardware ou software, que se destinem a ser utilizados para a prestação de serviços de confiança
Selo Eletrónico	Dados em formato eletrónico apenso ou logicamente associado a outros dados em formato eletrónico para garantir a origem e a integridade destes últimos
Selo Eletrónico Avançado	Selo eletrónico que obedeça aos requisitos: a) Esteja associado de modo único ao seu criador b) Permita identificar o seu criador c) Seja criado através dos dados de criação de selos eletrónicos cujo criador pode, com um elevado nível de confiança e sob o seu controlo, utilizar para a criação de um selo eletrónico, e d) Esteja ligado aos dados a que diz respeito de tal modo que seja detetável qualquer alteração posterior dos dados
Selo Eletrónico Qualificado	Selo eletrónico avançado criado por um dispositivo qualificado de criação de selos eletrónicos e que se baseie num certificado qualificado de selo eletrónico
Selo Temporal Qualificado	Selo temporal que satisfaça os requisitos: a) Vincular a data e a hora aos dados de forma a tornar razoavelmente impossível a alteração dos dados de forma não detetável, b) Basear-se numa fonte horária precisa ligada à Hora Universal Coordenada, e c) Ser assinado utilizando uma assinatura eletrónica avançada ou um selo eletrónico avançado do prestador qualificado de serviços de confiança, ou por outro método equivalente
Selos Temporais	Dados em formato eletrónico que vinculam outros dados em formato eletrónico a uma hora específica, criando uma prova de que esses outros dados existiam nesse momento
Serviço de Confiança	Serviço eletrónico geralmente prestado mediante remuneração, que consiste: a) Na criação, verificação e validação de assinaturas eletrónicas, selos eletrónicos ou selos temporais, serviços de envio registado eletrónico e certificados relacionados com estes serviços, ou b) Na criação, verificação e validação de certificados para a autenticação de sítios web, ou c) Na preservação das assinaturas, selos ou certificados eletrónicos relacionados com esses serviços
Serviço de Confiança Qualificado	Serviço de confiança que satisfaça os requisitos aplicáveis estabelecidos no Regulamento europeu 910/2014

Definições	
Termo	**Definição**
Serviço de Envio Registado Eletrónico	Serviço que torne possível a transmissão de dados entre terceiros por meios eletrónicos e forneça prova do tratamento dos dados transmitidos, nomeadamente a prova do envio e da receção dos mesmos, e que proteja os dados transferidos contra o risco de perda, roubo, dano ou alteração não autorizada
Serviço Qualificado de Envio Registado Eletrónico	Serviço de envio registado eletrónico que satisfaça os requisitos: a) Serem efetuados por um ou mais prestadores qualificados de serviços de confiança b) Garantirem, com um elevado nível de confiança, a identificação do remetente c) Garantir a identificação do destinatário antes da entrega dos dados d) O envio e a receção dos dados serem securizados por uma assinatura eletrónica avançada ou um selo eletrónico avançado do prestador qualificado de serviços de confiança, de modo a tornar impossível a alteração dos dados de forma não detetável e) Qualquer alteração a que devam ser sujeitos para o seu envio ou receção ser claramente indicada ao remetente e ao destinatário dos dados f) A data e a hora do envio e da receção, assim como as eventuais alterações dos dados, serem indicadas por meio de um selo temporal qualificado
Signatário	Pessoa singular que cria uma assinatura eletrónica.
Sistema de Identificação Eletrónica	Sistema de identificação eletrónica ao abrigo do qual sejam produzidos meios de identificação eletrónica para as pessoas singulares ou coletivas, ou para as pessoas singulares que representem pessoas coletivas
Titular	Ver Signatário.
Utilizador	Pessoa singular ou coletiva que utiliza a identificação eletrónica ou o serviço de confiança
Validação	Processo pelo qual é verificada e confirmada a validade de uma assinatura ou selo eletrónico
Validação Cronológica	Declaração de uma EVC que atesta a data e hora da criação, expedição ou receção de um documento eletrónico
Zona de Alta Segurança	Área de acesso controlado através de um ponto de entrada e limitada a pessoal autorizado devidamente credenciado e a visitantes devidamente acompanhados. As zonas de alta segurança devem estar encerradas em todo o seu perímetro e ser vigiadas 24 horas por dia, 7 dias por semana, por pessoal de segurança, por outro pessoal ou por meios eletrónicos